FTOS Command Line Reference Guide for the S5000 Switch

FTOS 9.0(1.3)

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2013 Dell Inc.

Trademarks used in this text: Dell™, the Dell logo, Dell Boomi™, Dell Precision™ , OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation.

2013–08

Contents

1 About this Guide..45

Objectives..45

Audience..45

Conventions..45

Information Icons..46

2 CLI Basics..47

Accessing the Command Line..47

Multiple Configuration Users..47

Navigating the CLI..48

Obtaining Help..48

Using the Keyword no Command..50

Filtering show Commands..50

Command Modes..51

Determining Chassis Mode..57

3 File Management..59

cd..59

copy..59

copy running-config startup-config..61

delete..61

dir..62

format flash..62

format usbflash..63

logging coredump..64

logging coredump server..64

pwd..65

rename..65

show file..66

show file-systems..67

show os-version..68

show running-config..70

show stack-unit..74

show startup-config..74

show version..75

upgrade boot (standalone unit)..76

upgrade system (standalone unit)..79

4 Control and Monitoring.. 81
asf-mode...81
banner exec..82
banner login..83
banner motd..84
cam-audit stack-unit..84
clear alarms..85
clear command history..85
clear line...86
configure...86
debug cpu-traffic-stats...87
debug ftpserver...87
disable..88
do..88
enable...89
enable optic-info-update interval...89
end...90
exec-banner..91
exec-timeout...91
exit..92
ftp-server enable...92
ftp-server topdir...93
ftp-server username..94
hostname..94
ip ftp password..95
ip ftp source-interface..95
ip ftp username..96
ip telnet server enable...97
ip telnet source-interface...97
ip tftp source-interface...98
line..99
motd-banner..99
ping...100
reload..102
send..103
service timestamps...103
show alarms..104
show command-history...105
show command-tree..105
show cpu-traffic-stats..108
show debugging..109

show environment..110
show inventory..111
show processes cpu..113
show processes ipc flow-control..116
show memory..118
show processes memory..118
show software ifm..122
show system..124
show tech-support..128
telnet..132
terminal length..133
traceroute..133
undebug all..135
write..136

5 802.1ag..137

ccm disable..137
ccm transmit-interval..137
clear ethernet cfm traceroute-cache..138
database hold-time..138
disable..138
domain..139
ethernet cfm..139
ethernet cfm mep..139
ethernet cfm mip..140
mep cross-check..141
mep cross-check enable..141
mep cross-check start-delay..141
ping ethernet..142
service..143
show ethernet cfm domain..143
show ethernet cfm maintenance-points local..144
show ethernet cfm maintenance-points remote..144
show ethernet cfm mipbd..145
show ethernet cfm port-statistics..145
show ethernet cfm statistics..146
show ethernet cfm traceroute-cache..147
traceroute cache hold-time..148
traceroute cache size..148
traceroute ethernet..148

6 802.1X..151

debug dot1x.......... 152
dot1x auth-fail-vlan.......... 152
dot1x auth-server.......... 153
dot1x auth-type mab-only.......... 153
dot1x authentication (Configuration).......... 154
dot1x authentication (Interface).......... 154
dot1x guest-vlan.......... 155
dot1x host-mode.......... 156
dot1x mac-auth-bypass.......... 156
dot1x max-eap-req.......... 157
dot1x max-supplicants.......... 157
dot1x port-control.......... 158
dot1x quiet-period.......... 158
dot1x reauthentication.......... 159
dot1x reauth-max.......... 159
dot1x server-timeout.......... 160
dot1x supplicant-timeout.......... 160
dot1x tx-period.......... 161
show dot1x cos-mapping interface.......... 161
show dot1x interface.......... 163

7 Boot User Mode.......... 165

boot change.......... 165
boot messages disable.......... 165
boot messages enable.......... 166
boot show net config retries.......... 166
boot write net config retries.......... 167
boot zero.......... 167
default gateway.......... 167
enable.......... 168
help.......... 168
ignore enable password.......... 169
ignore startup config.......... 170
interface management ethernet ip address.......... 170
interface management port config.......... 170
no default-gateway.......... 171
no interface management ethernet ip address.......... 171
reload.......... 172
show boot blc.......... 172
show boot selection.......... 172
show bootflash.......... 173
show bootvar.......... 173

show default-gateway....174
show interface management ethernet....174
show interface management port config....175

8 Access Control Lists (ACL)....177
Commands Common to all ACL Types....177
description....177
remark....178
show config....179
Common IP ACL Commands....179
access-class....180
clear counters ip access-group....180
ip access-group....180
show ip access-lists....181
show ip accounting access-list....182
Standard IP ACL Commands....183
deny....183
ip access-list standard....185
permit....185
resequence access-list....187
resequence prefix-list ipv4....188
seq....188
Extended IP ACL Commands....190
deny....190
deny tcp....192
deny udp....194
ip access-list extended....197
permit....197
permit tcp....199
permit udp....202
resequence access-list....204
resequence prefix-list ipv4....205
seq....206
Common MAC Access List Commands....208
clear counters mac access-group....208
mac access-group....209
show mac access-lists....209
show mac accounting access-list....210
Standard MAC ACL Commands....211
deny....211
mac access-list standard....212
permit....213

seq..214
Extended MAC ACL Commands..215
deny...216
mac access-list extended..217
permit..218
seq..220
IP Prefix List Commands..221
clear ip prefix-list...221
deny...222
ip prefix-list..222
permit..223
seq..224
show config..225
show ip prefix-list detail...225
show ip prefix-list summary..226
Route Map Commands...226
continue...227
description..228
match as-path..228
match community...229
match interface...229
match ip address...230
match ip next-hop..231
match ip route-source...231
match metric...232
match route-type...232
match tag..233
route-map..234
set as-path...235
set automatic-tag...235
set comm-list delete...236
set community...236
set level...237
set local-preference...238
set metric..239
set metric-type..239
set next-hop..240
set origin...241
set tag...241
set weight...242
show config...242
show route-map...243

AS-Path Commands....243
ip as-path access-list....243
show ip as-path-access-lists....244
IP Community List Commands....244
ip community-list....245
show ip community-lists....245

9 Bidirectional Forwarding Detection (BFD)....247

bfd all-neighbors....247
bfd enable (Configuration)....248
bfd enable (Interface)....249
bfd protocol-liveness....249
neighbor bfd....249
neighbor bfd disable....250
show bfd neighbors....251

10 Border Gateway Protocol IPv4 (BGPv4)....253

BGPv4 Commands....253
address-family....253
aggregate-address....254
bgp add-path....255
bgp always-compare-med....256
bgp asnotation....256
bgp bestpath as-path ignore....257
bgp bestpath as-path multipath-relax....257
bgp bestpath med confed....258
bgp bestpath med missing-as-best....258
bgp bestpath router-id ignore....259
bgp client-to-client reflection....259
bgp cluster-id....260
bgp confederation identifier....261
bgp confederation peers....261
bgp dampening....262
bgp default local-preference....263
bgp enforce-first-as....264
bgp fast-external-failover....264
bgp four-octet-as-support....265
bgp graceful-restart....265
bgp log-neighbor-changes....266
bgp non-deterministic-med....266
bgp recursive-bgp-next-hop....267
bgp regex-eval-optz-disable....268

bgp router-id......269
bgp soft-reconfig-backup......269
capture bgp-pdu max-buffer-size......270
capture bgp-pdu neighbor......270
clear ip bgp......271
clear ip bgp dampening......272
clear ip bgp flap-statistics......272
clear ip bgp peer-group......273
debug ip bgp......274
debug ip bgp dampening......275
debug ip bgp events......275
debug ip bgp keepalives......276
debug ip bgp notifications......276
debug ip bgp peer-group updates......277
debug ip bgp soft-reconfiguration......278
debug ip bgp updates......278
default-metric......279
description......279
distance bgp......280
max-paths......281
neighbor activate......281
neighbor add-path......282
neighbor advertisement-interval......283
neighbor advertisement-start......283
neighbor allowas-in......284
neighbor default-originate......284
neighbor description......285
neighbor distribute-list......286
neighbor ebgp-multihop......286
neighbor fail-over......287
neighbor filter-list......288
neighbor graceful-restart......288
neighbor local-as......289
neighbor maximum-prefix......290
neighbor next-hop-self......291
neighbor password......291
neighbor peer-group (assigning peers)......292
neighbor peer-group (creating group)......293
neighbor peer-group passive......294
neighbor remote-as......295
neighbor remove-private-as......295
neighbor route-map......296

neighbor route-reflector-client....297
neighbor send-community....298
neighbor shutdown....298
neighbor soft-reconfiguration inbound....299
neighbor subnet....300
neighbor timers....300
neighbor update-source....301
neighbor weight....302
network....302
network backdoor....303
redistribute....304
router bgp....305
show capture bgp-pdu neighbor....306
show config....307
show ip bgp....307
show ip bgp cluster-list....309
show ip bgp community....310
show ip bgp community-list....312
show ip bgp dampened-paths....313
show ip bgp detail....314
show ip bgp extcommunity-list....316
show ip bgp filter-list....316
show ip bgp flap-statistics....318
show ip bgp inconsistent-as....319
show ip bgp neighbors....320
show ip bgp next-hop....324
show ip bgp paths....325
show ip bgp paths as-path....327
show ip bgp paths community....328
show ip bgp peer-group....329
show ip bgp regexp....331
show ip bgp summary....333
show running-config bgp....335
timers bgp....335
MBGP Commands....335
address family ipv4 multicast (MBGP)....336
aggregate-address....336
bgp dampening....337
clear ip bgp ipv4 multicast....338
clear ip bgp dampening....339
clear ip bgp flap-statistics....339
debug ip bgp dampening....340

clear ip bgp peer-group....................340
debug ip bgp updates....................341
distance bgp....................341
neighbor activate....................342
neighbor advertisement-interval....................343
neighbor default-originate....................343
neighbor distribute-list....................344
neighbor filter-list....................345
neighbor maximum-prefix....................346
neighbor next-hop-self....................346
neighbor remove-private-as....................347
neighbor route-map....................347
neighbor route-reflector-client....................348
network....................349
redistribute....................350
redistribute ospf....................351
show ip bgp ipv4 multicast....................351
show ip bgp cluster-list....................353
show ip bgp community....................353
show ip bgp community-list....................354
show ip bgp dampened-paths....................354
show ip bgp filter-list....................355
show ip bgp flap-statistics....................356
show ip bgp inconsistent-as....................357
show ip bgp ipv4 multicast neighbors....................357
show ip bgp peer-group....................360
show ip bgp summary....................360
BGP Extended Communities (RFC 4360)....................362
deny....................362
deny regex....................363
description....................364
ip extcommunity-list....................364
match extcommunity....................365
permit....................365
permit regex....................366
set extcommunity rt....................367
set extcommunity soo....................368
show ip bgp ipv4 extcommunity-list....................369
show ip bgp paths extcommunity....................370
show ip extcommunity-list....................370
show running-config extcommunity-list....................371

11 Bare Metal Provisioning (BMP)........373
reload type........373
show reload-type........374
stop jump-start........375

12 Content Addressable Memory (CAM)........377
CAM Profile Commands........377
cam-acl (Configuration)........377
cam-acl-egress (Configuration)........378
cam-optimization........379
test cam-usage........380

13 Control Plane Policing (CoPP)........383
control-plane-cpuqos........383
service-policy rate-limit-cpu-queues........383
service-policy rate-limit-protocols........384
show cpu-queue rate cp........384
show ip protocol-queue-mapping........385
show ipv6 protocol-queue-mapping........386
show mac protocol-queue-mapping........386

14 Data Center Bridging (DCB)........389
DCB Command........389
advertise dcbx-appln-tlv........389
advertise dcbx-tlv........390
clear ets counters........391
clear pfc counters........391
dcb enable........392
dcb-map........392
dcb-map stack-unit all stack-ports all........393
dcbx port-role........394
dcbx version........394
debug dcbx........395
fcoe priority-bits........396
iscsi priority-bits........396
pfc mode on........397
pfc no-drop queues........397
pfc priority........398
priority-group bandwidth pfc........399
priority-pgid........400
show dcb........401

show qos dcb-map... 402
show interfaces dcbx detail... 403
show interfaces ets.. 406
show interfaces pfc...410
show interfaces pfc statistics..413
show stack-unit stack-ports ets detail.. 414
show stack-unit stack-ports pfc detail...415

15 Dynamic Host Configuration Protocol (DHCP).. 417

Commands to Configure the System to be a DHCP Server...417
clear ip dhcp...417
debug ip dhcp server...418
default-router...418
disable..419
dns-server...419
domain-name..419
excluded-address..420
hardware-address..420
host... 421
lease.. 421
netbios-name-server... 422
netbios-node-type..422
network...423
pool... 423
show ip dhcp binding..423
show ip dhcp configuration.. 424
show ip dhcp conflict..424
show ip dhcp server.. 425
Commands to Configure Secure DHCP...425
arp inspection.. 425
arp inspection-trust.. 426
clear ip dhcp snooping.. 426
ip dhcp relay... 426
ip dhcp snooping...427
ip dhcp snooping binding...427
ip dhcp snooping database...428
ip dhcp snooping database renew.. 429
ip dhcp snooping trust.. 429
ip dhcp source-address-validation..429
ip dhcp snooping vlan...430
ip dhcp snooping verify mac-address... 430
show ip dhcp snooping..431

16 Equal Cost Multi-Path Overview (ECMP)....................433
- ecmp-group....................433
- hash-algorithm....................434
- hash-algorithm ecmp....................435
- ip ecmp-group....................436
- link-bundle-distribution trigger-threshold....................436
- link-bundle-monitor enable....................437

17 FCoE Transit....................439
- clear fip-snooping database interface vlan....................439
- clear fip-snooping statistics....................440
- debug fip snooping....................440
- feature fip-snooping....................441
- fip-snooping enable....................441
- fip-snooping fc-map....................442
- fip-snooping max-sessions-per-enodemac....................442
- fip-snooping port-mode fcf....................443
- show fip-snooping config....................443
- show fip-snooping enode....................444
- show fip-snooping fcf....................445
- show fip-snooping sessions....................446
- show fip-snooping statistics....................447
- show fip-snooping system....................450
- show fip-snooping vlan....................450

18 Force10 Resilient Ring Protocol (FRRP)....................451
- clear frrp....................451
- debug frrp....................452
- member-vlan....................453
- mode....................453
- protocol frrp....................454
- show frrp....................454

19 GARP VLAN Registration (GVRP)....................457
- clear gvrp statistics....................458
- debug gvrp....................458
- disable....................459
- garp timers....................460
- gvrp enable....................461
- gvrp registration....................461
- protocol gvrp....................462

show config 462
show garp timers 463
show gvrp 463
show gvrp statistics 464

20 High Availability (HA) 467
redundancy disable-auto-reboot 467
redundancy force-failover 468
redundancy protocol 468
redundancy reset-counter 469
redundancy synchronize 469
show redundancy 470

21 Internet Group Management Protocol (IGMP) 473
IGMP Commands 473
clear ip igmp groups 473
debug ip igmp 474
ip igmp access-group 475
ip igmp group-join-limit 475
ip igmp immediate-leave 476
ip igmp last-member-query-interval 476
ip igmp querier-timeout 477
ip igmp query-interval 477
ip igmp query-max-resp-time 478
ip igmp ssm-map 478
ip igmp static-group 479
ip igmp version 480
show ip igmp groups 480
show ip igmp interface 482
show ip igmp ssm-map 483
IGMP Snooping Commands 484
ip igmp snooping enable 484
ip igmp snooping fast-leave 485
ip igmp snooping flood 486
ip igmp snooping last-member-query-interval 486
ip igmp snooping mrouter 487
ip igmp snooping querier 487
show ip igmp snooping mrouter 488

22 Interfaces 489
Basic Interface Commands 489
clear counters 489

clear dampening....490
cx4-cable-length....491
dampening....492
description....493
duplex (Management interface)....494
ecmp-group....495
flowcontrol....495
interface....497
interface loopback....499
interface ManagementEthernet....499
interface null....500
interface range....501
interface range macro (define)....503
interface range macro name....504
interface vlan....505
keepalive....506
monitor interface....506
mtu....509
portmode hybrid....510
rate-interval....511
show config....512
show config (from INTERFACE RANGE mode)....512
show interfaces....513
show interfaces configured....517
show interfaces dampening....518
show interfaces description....519
show interfaces stack-unit....521
show interfaces status....522
show interfaces switchport....524
show interfaces transceiver....525
show range....530
show running-config ecmp-group....531
shutdown....531
speed (Management interface)....532
stack-unit portmode....533
switchport....533
Port Channel Commands....534
channel-member....535
group....536
interface port-channel....536
minimum-links....537
port-channel failover-group....538

show config 538
show interfaces port-channel 539
show port-channel-flow 542
UDP Broadcast 543
debug ip udp-helper 544
ip udp-broadcast-address 544
ip udp-helper udp-port 545
show ip udp-helper 546
Fibre Channel Interface Commands 546
change fc-trace-level 546
clear counters fibrechannel 547
create fc-dump-support 548
fabric 548
feature fc 549
interface fibrechannel 549
show fc-trace-level 551
show interfaces fibrechannel 551
show fc switch 556
speed 556

23 IPv4 Routing 559
arp 559
arp learn-enable 560
arp retries 560
arp timeout 561
clear arp-cache 561
clear host 562
clear ip fib stack-unit 562
clear ip route 563
clear tcp statistics 563
debug arp 564
debug ip dhcp 565
debug ip icmp 566
debug ip packet 567
ip address 569
ip directed-broadcast 570
ip domain-list 570
ip domain-lookup 571
ip domain-name 572
ip helper-address 572
ip helper-address hop-count disable 573
ip host 574

ip max-frag-count.....574
ip mtu.....575
ip name-server.....576
ip proxy-arp.....577
ip route.....577
ip source-route.....578
ip unreachables.....579
load balance.....579
management route.....581
show arp.....581
show arp retries.....584
show hosts.....584
show ip cam stack-unit.....586
show ip fib stack-unit.....588
show ip flow.....589
show ip interface.....590
show ip management-route.....592
show ipv6 management-route.....593
show ip protocols.....594
show ip route.....594
show ip route list.....597
show ip route summary.....598
show ip traffic.....599
show tcp statistics.....601

24 IPv6 Access Control Lists (IPv6 ACLs).....603

IPv6 ACL Commands.....603
cam-acl.....603
cam-acl-egress.....604
clear counters ipv6 access-group.....605
deny.....606
deny icmp.....606
deny tcp.....608
deny udp.....610
ipv6 access-group.....612
ipv6 control-plane egress-filter.....613
ipv6 access-list.....613
permit.....614
permit icmp.....615
permit tcp.....616
permit udp.....618
remark.....620

resequence access-list....621
resequence prefix-list ipv6....621
seq....622
show cam-acl....624
show cam-acl-egress....625
show config....625
show ipv6 accounting access-list....626
show running-config acl....627
test cam-usage....628
IPv6 Route Map Commands....629
match ipv6 address....629
match ipv6 next-hop....630
match ipv6 route-source....630
route-map....631
set ipv6 next-hop....631
show config....632
show route-map....632

25 IPv6 Basics....635
clear ipv6 fib....635
clear ipv6 route....635
clear ipv6 mld_host....636
ipv6 address autoconfig....636
ipv6 address....636
ipv6 control-plane icmp error-rate-limit....637
ipv6 flowlabel-zero....638
ipv6 host....638
ipv6 name-server....639
ipv6 nd dad attempts....639
ipv6 nd prefix....640
ipv6 route....641
show ipv6 cam stack-unit....643
show ipv6 control-plane icmp....644
show ipv6 fib stack-unit....644
show ipv6 flowlabel-zero....645
show ipv6 interface....645
show ipv6 mld_host....647
show ipv6 route....648
trust ipv6-diffserv....650

26 IPv6 Border Gateway Protocol (IPv6 BGP)....651
IPv6 BGP Commands....651

aggregate-address.......651
bgp always-compare-med.......652
bgp bestpath as-path ignore.......653
bgp bestpath med confed.......653
bgp bestpath med missing-as-best.......654
bgp client-to-client reflection.......654
bgp cluster-id.......655
bgp confederation identifier.......655
bgp confederation peers.......656
bgp dampening.......657
bgp default local-preference.......658
bgp enforce-first-as.......658
bgp fast-external-failover.......659
bgp four-octet-as-support.......659
bgp graceful-restart.......660
bgp log-neighbor-changes.......661
bgp non-deterministic-med.......661
bgp recursive-bgp-next-hop.......662
bgp regex-eval-optz-disable.......662
bgp router-id.......663
bgp soft-reconfig-backup.......664
capture bgp-pdu max-buffer-size.......664
capture bgp-pdu neighbor (ipv6).......665
clear ip bgp * (asterisk).......665
clear ip bgp as-number.......666
clear ip bgp ipv6-address.......667
clear ip bgp peer-group.......668
clear ip bgp ipv6 dampening.......668
clear ip bgp ipv6 flap-statistics.......669
clear ip bgp ipv6 unicast soft.......670
debug ip bgp.......671
debug ip bgp events.......672
debug ip bgp ipv6 dampening.......672
debug ip bgp ipv6 unicast soft-reconfiguration.......673
debug ip bgp keepalives.......674
debug ip bgp notifications.......674
debug ip bgp updates.......675
default-metric.......676
description.......676
distance bgp.......677
maximum-paths.......678
neighbor activate.......678

neighbor advertisement-interval....679
neighbor allowas-in....680
neighbor default-originate....680
neighbor description....681
neighbor distribute-list....682
neighbor ebgp-multihop....682
neighbor fall-over....683
neighbor filter-list....684
neighbor maximum-prefix....684
neighbor next-hop-self....685
neighbor peer-group (assigning peers)....686
neighbor peer-group (creating group)....687
neighbor peer-group passive....687
neighbor remote-as....688
neighbor remove-private-as....689
neighbor route-map....689
neighbor route-reflector-client....690
neighbor send-community....691
neighbor shutdown....691
neighbor soft-reconfiguration inbound....692
neighbor subnet....693
neighbor timers....693
neighbor update-source....694
neighbor weight....695
neighbor X:X:X::X password....696
network....696
network backdoor....697
redistribute....698
redistribute isis....699
redistribute ospf....700
router bgp....701
show capture bgp-pdu neighbor....701
show config....702
show ip bgp ipv6 unicast....702
show ip bgp ipv6 unicast cluster-list....703
show ip bgp ipv6 unicast community....703
show ip bgp ipv6 unicast community-list....704
show ip bgp ipv6 unicast dampened-paths....705
show ip bgp ipv6 unicast detail....705
show ip bgp ipv6 unicast extcommunity-list....705
show ip bgp ipv6 unicast filter-list....706
show ip bgp ipv6 unicast flap-statistics....706

show ip bgp ipv6 unicast inconsistent-as....707
show ip bgp ipv6 unicast neighbors....708
show ip bgp ipv6 unicast peer-group....711
show ip bgp ipv6 unicast summary....712
show ip bgp next-hop....713
show ip bgp paths....713
show ip bgp paths as-path....714
show ip bgp paths community....715
show ip bgp paths extcommunity....715
show ip bgp regexp....715
timers bgp....716
IPv6 MBGP Commands....717
address family....717
aggregate-address....717
bgp dampening....718
clear ip bgp ipv6 unicast....719
clear ip bgp ipv6 unicast dampening....720
clear ip bgp ipv6 flap-statistics....720
debug ip bgp ipv6 unicast dampening....721
debug ip bgp ipv6 unicast peer-group updates....722
debug ip bgp ipv6 unicast updates....722
distance bgp....723
neighbor activate....724
neighbor advertisement-interval....724
neighbor default-originate....725
neighbor distribute-list....726
neighbor filter-list....726
neighbor maximum-prefix....727
neighbor next-hop-self....728
neighbor remove-private-as....728
neighbor route-map....729
neighbor route-reflector-client....730
network....730
redistribute....731
show ip bgp ipv6 unicast....732
show ip bgp ipv6 unicast cluster-list....734
show ip bgp ipv6 unicast community....734
show ip bgp ipv6 unicast community-list....735
show ip bgp ipv6 unicast dampened-paths....735
show ip bgp ipv6 unicast detail....736
show ip bgp ipv6 unicast filter-list....736
show ip bgp ipv6 unicast flap-statistics....737

show ip bgp ipv6 unicast inconsistent-as....738
show ip bgp ipv6 unicast neighbors....738
show ip bgp ipv6 unicast peer-group....742
show ip bgp ipv6 unicast summary....742
iscsi aging time....744

27 iSCSI Optimization....745
advertise dcbx-app-tlv....745
iscsi aging time....745
iscsi cos....746
iscsi enable....747
iscsi priority-bits....747
iscsi profile-compellant....747
iscsi target port....748
show iscsi....748
show iscsi session....749
show iscsi session detailed....750
show run iscsi....751

28 Intermediate System to Intermediate System (IS-IS)....753
adjacency-check....753
advertise....754
area-password....754
clear config....755
clear isis....756
clns host....756
debug isis....757
debug isis adj-packets....757
debug isis local-updates....758
debug isis snp-packets....758
debug isis spf-triggers....759
debug isis update-packets....759
default-information originate....760
description....761
distance....761
distribute-list in....762
distribute-list out....763
distribute-list redistributed-override....764
domain-password....764
graceful-restart ietf....765
graceful-restart interval....766
graceful-restart t1....766

graceful-restart t2 767
graceful-restart t3 767
graceful-restart restart-wait 768
hello padding 769
hostname dynamic 769
ignore-lsp-errors 770
ip router isis 770
ipv6 router isis 771
isis circuit-type 772
isis csnp-interval 772
isis hello-interval 773
isis hello-multiplier 774
isis hello padding 774
isis ipv6 metric 775
isis metric 776
isis network point-to-point 776
isis password 777
isis priority 777
is-type 778
log-adjacency-changes 779
lsp-gen-interval 779
lsp-mtu 780
lsp-refresh-interval 781
max-area-addresses 781
max-lsp-lifetime 782
maximum-paths 782
metric-style 783
multi-topology 784
net 784
passive-interface 785
redistribute 785
redistribute bgp 787
redistribute ospf 788
router isis 790
set-overload-bit 790
show config 791
show isis database 792
show isis graceful-restart detail 794
show isis hostname 795
show isis interface 795
show isis neighbors 796
show isis protocol 798

show isis traffic....................799
spf-interval....................801

29 Link Aggregation Control Protocol (LACP)....................803
clear lacp counters....................803
debug lacp....................803
lacp long-timeout....................804
lacp port-priority....................805
lacp system-priority....................805
port-channel mode....................806
port-channel-protocol lacp....................807
show lacp....................807

30 Layer 2....................809
MAC Addressing Commands....................809
clear mac-address-table dynamic....................809
mac-address-table aging-time....................810
mac-address-table static....................810
mac-address-table station-move threshold....................811
mac-address-table station-move refresh-arp....................812
mac learning-limit....................812
mac learning-limit learn-limit-violation....................813
mac learning-limit mac-address-sticky....................814
mac learning-limit station-move-violation....................815
mac learning-limit reset....................815
show cam mac stack-unit....................816
show mac-address-table....................817
show mac-address-table aging-time....................819
show mac accounting access-list....................820
show mac learning-limit....................821
Virtual LAN (VLAN) Commands....................822
description....................822
default vlan-id....................822
default-vlan disable....................823
name....................823
show config....................824
show vlan....................824
tagged....................827
track ip....................828
untagged....................829
Far-End Failure Detection (FEFD)....................830
debug fefd....................830

fefd....831
fefd disable....831
fefd-global....832
fefd-global interval....832
fefd interval....833
fefd mode....833
fefd reset....834
show fefd....835

31 Link Layer Discovery Protocol (LLDP)....837
LLPD Commands....837
advertise dot1-tlv....837
advertise dot3-tlv....838
advertise management-tlv....838
clear lldp counters....839
clear lldp neighbors....840
debug lldp interface....840
disable....841
hello....842
mode....842
multiplier....843
protocol lldp (Configuration)....843
protocol lldp (Interface)....843
show lldp neighbors....844
show lldp statistics....845
show running-config lldp....845
LLDP-MED Commands....846
advertise med guest-voice....846
advertise med guest-voice-signaling....847
advertise med location-identification....848
advertise med power-via-mdi....848
advertise med softphone-voice....849
advertise med streaming-video....850
advertise med video-conferencing....850
advertise med video-signaling....851
advertise med voice....851
advertise med voice-signaling....852

32 Multicast Source Discovery Protocol (MSDP)....853
debug ip msdp....853
ip msdp cache-rejected-sa....853
ip msdp default-peer....854

ip msdp log-adjacency-changes......855
ip msdp mesh-group......855
ip msdp originator-id......856
ip msdp peer......856
ip msdp redistribute......858
ip msdp sa-filter......858
ip msdp sa-limit......859
ip msdp shutdown......859
ip multicast-msdp......860
show ip msdp......860

33 Multiple Spanning Tree Protocol (MSTP)......863
debug spanning-tree mstp......863
description......864
disable......864
forward-delay......865
hello-time......865
max-age......866
max-hops......866
msti......867
name......868
protocol spanning-tree mstp......868
revision......869
show config......869
show spanning-tree mst configuration......870
show spanning-tree msti......870
spanning-tree......873
spanning-tree msti......873
spanning-tree mstp......874
tc-flush-standard......875

34 Multicast......877
IPv4 Multicast Commands......877
clear ip mroute......877
ip mroute......878
ip multicast-limit......879
ip multicast-routing......879
show ip mroute......880
show ip rpf......882
IPv6 Multicast Commands......882
ip multicast-limit......882

35 Neighbor Discovery Protocol (NDP)....885
clear ipv6 neighbors....885
ipv6 nd mtu....886
ipv6 neighbor....887
show ipv6 neighbors....888

36 NPIV Proxy Gateway....891
dcb-map....891
description....892
fabric....892
fabric-id vlan....893
fc-map....894
fcf-priority....895
fcoe-map....895
feature fc....896
fka-adv-period....897
interface vlan (NPIV proxy gateway)....897
keepalive....898
priority-pgid....899
priority-group bandwidth pfc....900
show fcoe-map....901
show npiv devices....903
show fc switch....905
show qos dcb-map....906

37 Open Shortest Path First (OSPFv2)....909
area default-cost....909
area nssa....910
area range....910
area stub....911
area virtual-link....912
auto-cost....913
clear ip ospf....914
clear ip ospf statistics....914
debug ip ospf....915
default-information originate....917
default-metric....918
description....918
distance....919
distance ospf....919
distribute-list in....920

distribute-list out....921
fast-convergence....922
flood-2328....922
graceful-restart grace-period....923
graceful-restart helper-reject....923
graceful-restart mode....924
graceful-restart role....924
ip ospf auth-change-wait-time....925
ip ospf authentication-key....925
ip ospf cost....926
ip ospf dead-interval....926
ip ospf hello-interval....927
ip ospf message-digest-key....927
ip ospf mtu-ignore....928
ip ospf network....928
ip ospf priority....929
ip ospf retransmit-interval....929
ip ospf transmit-delay....930
log-adjacency-changes....930
maximum-paths....931
mib-binding....931
network area....932
passive-interface....932
debug ip ospf....934
redistribute bgp....936
redistribute isis....937
router-id....938
router ospf....938
show config....939
show ip ospf....939
show ip ospf asbr....941
show ip ospf database....941
show ip ospf database asbr-summary....943
show ip ospf database external....944
show ip ospf database network....946
show ip ospf database nssa-external....948
show ip ospf database opaque-area....949
show ip ospf database opaque-as....950
show ip ospf database opaque-link....951
show ip ospf database router....952
show ip ospf database summary....954
show ip ospf interface....956

show ip ospf neighbor....958
show ip ospf routes....959
show ip ospf statistics....960
show ip ospf timers rate-limit....963
show ip ospf topology....963
show ip ospf virtual-links....964
summary-address....965
timers spf....966
timers throttle lsa all....967
timers throttle lsa arrival....967

38 Policy-based Routing (PBR)....969
description....969
ip redirect-group....970
ip redirect-list....970
permit....971
redirect....972
seq....974
show ip redirect-list....975

39 PIM-Sparse Mode (PIM-SM)....977
IPv4 PIM-Sparse Mode Commands....977
clear ip pim rp-mapping....977
clear ip pim tib....977
clear ip pim snooping tib....978
debug ip pim....978
ip pim bsr-border....979
ip pim bsr-candidate....980
ip pim dr-priority....981
ip pim graceful-restart....981
ip pim join-filter....982
ip pim ingress-interface-map....983
ip pim neighbor-filter....983
ip pim query-interval....984
ip pim register-filter....984
ip pim rp-address....985
ip pim rp-candidate....985
ip pim snooping....986
ip pim sparse-mode....987
ip pim sparse-mode sg-expiry-timer....988
ip pim spt-threshold....988
no ip pim snooping dr-flood....989

show ip pim bsr-router....989
show ip pim interface.... 990
show ip pim neighbor....991
show ip pim rp....992
show ip pim snooping interface....993
show ip pim snooping neighbor....994
show ip pim snooping tib.... 995
show ip pim summary.... 997
show ip pim tib....998
show running-config pim.... 1000
IPv6 PIM-Sparse Mode Commands....1000
clear ipv6 pim tib....1000
debug ipv6 pim.... 1001
ipv6 pim bsr-border....1002
ipv6 pim bsr-candidate.... 1003
ipv6 pim dr-priority....1003
ipv6 pim join-filter.... 1004
ipv6 pim query-interval.... 1005
ipv6 pim neighbor-filter....1005
ipv6 pim register-filter....1006
ipv6 pim rp-address.... 1006
ipv6 pim rp-candidate.... 1007
ipv6 pim sparse-mode....1008
ipv6 pim spt-threshold.... 1008
show ipv6 pim bsr-router....1009
show ipv6 pim interface....1009
show ipv6 pim neighbor.... 1010
show ipv6 pim rp....1010
show ipv6 pim tib.... 1011

40 PIM-Source Specific Mode (PIM-SSM).... 1013
IPv4 PIM Commands....1013
IPv4 PIM-Source Specific Mode Commands.... 1013
ip pim ssm-range.... 1014
show ip pim ssm-range....1014
IPv6 PIM Commands....1015
IPv6 PIM-Source Specific Mode Commands.... 1015

41 Port Monitoring....1017
description.... 1017
monitor session....1018
show config.... 1018

show monitor session....1019
show running-config monitor session....1020
source (port monitoring)....1021

42 Per-VLAN Spanning Tree Plus (PVST+)....1023

description....1023
disable....1023
extend system-id....1024
protocol spanning-tree pvst....1025
show spanning-tree pvst....1025
spanning-tree pvst....1028
spanning-tree pvst err-disable....1030
tc-flush-standard....1031
vlan bridge-priority....1031
vlan forward-delay....1032
vlan hello-time....1033
vlan max-age....1033

43 Quality of Service (QoS)....1035

Global Configuration Commands....1035
qos-rate-adjust....1035
Per-Port QoS Commands....1036
dot1p-priority....1036
rate police....1037
rate shape....1038
service-class dot1p-mapping....1038
service-class dynamic dot1p....1039
service-class bandwidth-weight....1040
strict-priority queue....1040
Policy-Based QoS Commands....1041
bandwidth-percentage....1041
class-map....1042
clear qos statistics....1043
description....1043
match ip access-group....1044
match ip dscp....1045
match ip precedence....1045
match mac access-group....1046
match mac dot1p....1047
match mac vlan....1047
policy-aggregate....1048
policy-map-input....1048

policy-map-output....1049
qos-policy-input....1050
qos-policy-output....1050
rate-police....1051
rate-shape....1052
service-policy input....1052
service-policy output....1053
service-queue....1054
set....1054
show qos class-map....1055
show qos dot1p-queue-mapping....1056
show qos policy-map....1056
show qos policy-map-input....1058
show qos policy-map-output....1059
show qos qos-policy-input....1059
show qos qos-policy-output....1060
show qos statistics....1060
show qos wred-profile....1062
test cam-usage....1063
trust....1065
wred....1066
wred-profile....1067

44 Private VLAN (PVLAN)....1069
ip local-proxy-arp....1070
private-vlan mode....1070
private-vlan mapping secondary-vlan....1071
show interfaces private-vlan....1072
show vlan private-vlan....1073
show vlan private-vlan mapping....1075
switchport mode private-vlan....1076

45 Routing Information Protocol (RIP)....1079
auto-summary....1079
clear ip rip....1079
debug ip rip....1080
default-information originate....1080
default-metric....1081
description....1082
distance....1082
distribute-list in....1083
distribute-list out....1084

ip poison-reverse....1085
ip rip receive version....1085
ip rip send version....1086
ip split-horizon....1086
maximum-paths....1087
neighbor....1087
network....1088
offset-list....1088
output-delay....1089
passive-interface....1090
redistribute....1090
redistribute isis....1091
redistribute ospf....1092
router rip....1093
show config....1093
show ip rip database....1094
show running-config rip....1095
timers basic....1095
version....1096

46 Remote Monitoring (RMON)....1097

rmon alarm....1097
rmon collection history....1098
rmon collection statistics....1099
rmon event....1100
rmon hc-alarm....1100
show rmon....1101
show rmon alarms....1102
show rmon events....1103
show rmon hc-alarm....1104
show rmon history....1105
show rmon log....1106
show rmon statistics....1106

47 Rapid Spanning Tree Protocol (RSTP)....1109

bridge-priority....1109
debug spanning-tree rstp....1109
description....1110
disable....1111
forward-delay....1111
hello-time....1112
max-age....1113

protocol spanning-tree rstp....1113
show config....1114
show spanning-tree rstp....1114
spanning-tree rstp....1116
tc-flush-standard....1118

48 Security....1119
AAA Accounting Commands....1119
aaa accounting....1119
aaa accounting suppress....1121
accounting....1121
show accounting....1122
Authorization and Privilege Commands....1122
aaa authorization commands....1122
aaa authorization config-commands....1123
aaa authorization exec....1123
authorization....1124
privilege level (CONFIGURATION mode)....1125
privilege level (LINE mode)....1126
Authentication and Password Commands....1126
aaa authentication enable....1126
aaa authentication login....1127
access-class....1129
enable password....1129
enable restricted....1130
enable secret....1131
login authentication....1132
password....1133
password-attributes....1133
privilege level (CONFIGURATION mode)....1134
privilege level (LINE mode)....1135
service password-encryption....1136
show privilege....1136
show users....1137
timeout login response....1138
username....1138
RADIUS Commands....1139
debug radius....1140
ip radius source-interface....1140
radius-server deadtime....1141
radius-server host....1141
radius-server key....1143

radius-server retransmit....1143
radius-server timeout....1144
TACACS+ Commands....1144
debug tacacs+....1145
ip tacacs source-interface....1145
tacacs-server host....1146
tacacs-server key....1147
Port Authentication (802.1X) Commands....1147
dot1x authentication (Configuration)....1148
dot1x authentication (Interface)....1148
dot1x auth-fail-vlan....1149
dot1x auth-server....1150
dot1x guest-vlan....1150
dot1x max-eap-req....1151
dot1x port-control....1151
dot1x quiet-period....1152
dot1x reauthentication....1152
dot1x reauth-max....1153
dot1x server-timeout....1153
dot1x supplicant-timeout....1154
dot1x tx-period....1154
show dot1x interface....1155
SSH Server and SCP Commands....1156
crypto key generate....1156
debug ip ssh....1157
ip scp topdir....1157
ip ssh authentication-retries....1158
ip ssh connection-rate-limit....1158
ip ssh hostbased-authentication....1159
ip ssh key-size....1159
ip ssh password-authentication....1160
ip ssh pub-key-file....1160
ip ssh rhostsfile....1161
ip ssh rsa-authentication (Config)....1162
ip ssh rsa-authentication (EXEC)....1163
ip ssh server....1163
show crypto....1164
show ip ssh....1165
show ip ssh client-pub-keys....1166
show ip ssh rsa-authentication....1166
ssh....1167
Secure DHCP Commands....1168

clear ip dhcp snooping.......... 1169
ip dhcp relay.......... 1169
ip dhcp snooping.......... 1169
ip dhcp snooping binding.......... 1170
ip dhcp snooping database.......... 1171
ip dhcp snooping database renew.......... 1171
ip dhcp snooping trust.......... 1172
ip dhcp source-address-validation.......... 1172
ip dhcp snooping vlan.......... 1172
show ip dhcp snooping.......... 1173

49 Service Provider Bridging.......... 1175
debug protocol-tunnel.......... 1175
protocol-tunnel.......... 1176
protocol-tunnel destination-mac.......... 1177
protocol-tunnel enable.......... 1177
protocol-tunnel rate-limit.......... 1178
show protocol-tunnel.......... 1178

50 sFlow.......... 1181
sflow collector.......... 1182
sflow enable (Global).......... 1183
sflow enable (Interface).......... 1183
sflow extended-switch enable.......... 1184
sflow polling-interval (Global).......... 1184
sflow polling-interval (Interface).......... 1185
sflow sample-rate (Global).......... 1185
sflow sample-rate (Interface).......... 1186
show sflow.......... 1186
show sflow stack-unit.......... 1188

51 Simple Network Management Protocol (SNMP) and Syslog.......... 1189
SNMP Commands.......... 1189
show snmp.......... 1190
show snmp engineID.......... 1190
show snmp group.......... 1191
show snmp user.......... 1192
snmp ifmib ifalias long.......... 1192
snmp-server community.......... 1193
snmp-server contact.......... 1195
snmp-server enable traps.......... 1195
snmp-server engineID.......... 1196

snmp-server group 1197
snmp-server host 1199
snmp-server location 1201
snmp-server packetsize 1202
snmp-server trap-source 1202
snmp-server user 1203
snmp-server view 1205
snmp trap link-status 1206
Syslog Commands 1206
clear logging 1206
default logging buffered 1207
default logging console 1207
default logging monitor 1208
default logging trap 1208
logging 1208
logging buffered 1209
logging console 1210
logging facility 1210
logging history 1212
logging history size 1212
logging monitor 1213
logging on 1213
logging source-interface 1214
logging synchronous 1215
logging trap 1216
show logging 1216
show logging driverlog stack-unit 1218
terminal monitor 1218

52 Spanning Tree Protocol (STP) 1221
bridge-priority 1221
debug spanning-tree 1221
description 1222
disable 1223
forward-delay 1223
hello-time 1224
max-age 1224
protocol spanning-tree 1225
show config 1225
show spanning-tree 0 1226
spanning-tree 0 1229

53 Stacking Commands..1231
redundancy disable-auto-reboot stack-unit...1231
redundancy force-failover stack-unit...1232
reset stack-unit...1232
show redundancy.. 1233
show system stack-ports..1234
show system stack-unit stack-group... 1236
stack-unit priority...1237
stack-unit provision.. 1237
stack-unit renumber... 1238
stack-unit stack-group...1239
upgrade boot (stack unit)..1239
upgrade system (stack unit).. 1242

54 Storm Control...1245
show storm-control broadcast.. 1245
show storm-control multicast...1246
show storm-control unknown-unicast... 1247
storm-control broadcast (Configuration)...1248
storm-control broadcast (Interface)..1248
storm-control multicast (Configuration).. 1249
storm-control multicast (Interface)... 1249
storm-control unknown-unicast (Configuration).. 1250
storm-control unknown-unicast (Interface)... 1250

55 System Time and Date...1253
calendar set... 1253
clock read-calendar... 1254
clock set...1254
clock summer-time date.. 1255
clock summer-time recurring... 1256
clock timezone... 1258
clock update-calendar..1258
debug ntp... 1259
ntp authenticate...1259
ntp authentication-key... 1260
ntp broadcast client... 1261
ntp disable... 1261
ntp multicast client.. 1261
ntp server...1262
ntp source.. 1263

ntp trusted-key....1263
ntp update-calendar....1264
show calendar....1264
show clock....1265
show ntp associations....1266
show ntp status....1267

56 Uplink Failure Detection (UFD)....1269
clear ufd-disable....1269
debug uplink-state-group....1270
description....1270
downstream....1271
downstream auto-recover....1272
downstream disable links....1272
enable....1273
show running-config uplink-state-group....1273
show uplink-state-group....1274
uplink-state-group....1276
upstream....1276

57 VLAN Stacking....1279
dei enable....1279
dei honor....1280
dei mark....1280
member....1281
show interfaces dei-honor....1282
show interfaces dei-mark....1283
stack-unit stack-group....1284
vlan-stack access....1284
vlan-stack compatible....1285
vlan-stack dot1p-mapping....1285
vlan-stack protocol-type....1286
vlan-stack trunk....1287

58 Virtual Link Trunking (VLT)....1289
back-up destination....1289
clear vlt statistics....1290
delay-restore....1290
lacp ungroup member-independent....1291
peer-link port-channel....1291
primary-priority....1292
show vlt....1292

show vlt backup-link 1293
show vlt counter 1294
show vlt role 1295
show vlt statistics 1295
show vlt statistics igmp-snoop 1296
system-mac 1297
unit-id 1298
vlt domain 1298
vlt-peer-lag port-channel 1299

59 Virtual Router Redundancy Protocol (VRRP) 1301

IPv4 VRRP Commands 1301
advertise-interval 1301
authentication-type 1302
clear counters vrrp 1302
debug vrrp 1303
description 1304
disable 1304
hold-time 1305
preempt 1305
priority 1306
show config 1306
show vrrp 1307
track 1310
virtual-address 1310
vrrp delay minimum 1311
vrrp delay reload 1312
vrrp-group 1313
IPv6 VRRP Commands 1313
clear counters vrrp ipv6 1314
debug vrrp ipv6 1314
show vrrp ipv6 1315
vrrp-ipv6-group 1317

60 Debugging and Diagnostics 1319

Offline Diagnostic Commands 1319
diag stack-unit 1319
offline stack-unit 1320
online stack-unit 1321
Buffer Tuning Commands 1322
buffer-profile (Configuration) 1322
show buffer-profile stack-unit 1323

Hardware Commands..1323
clear hardware stack-unit..1323
clear hardware system-flow..1324
hardware watchdog..1325
show hardware layer2 acl..1325
show hardware layer3...1326
show hardware stack-unit..1326
show hardware system-flow..1331

61 ICMP Message Types...1335

62 SNMP Traps...1337

1

About this Guide

This book provides information about the Dell Networking operating system (FTOS) command line interface (CLI). This book also includes information about the protocols and features found in FTOS.

References

For more information about your system, refer to the following documents:

- FTOS Configuration Guides
- Installation and Maintenance Guides
- Release Notes

Objectives

This book is intended as a reference guide for the FTOS CLI commands, with detailed syntax statements, along with usage information and sample output.

NOTE: For more information about when to use the CLI commands, refer to the FTOS Configuration Guide for your system.

Audience

This book is intended for system administrators who are responsible for configuring or maintaining networks. This guide assumes that you are knowledgeable in Layer 2 and Layer 3 networking technologies.

Conventions

This book uses the following conventions to describe command syntax.

`Keyword`	Keywords are in Currier and must be entered in the CLI as listed.
parameter	Parameters are in italics and require a number or word to be entered in the CLI.
{X}	Keywords and parameters within braces must be entered in the CLI.
[X]	Keywords and parameters within brackets are optional.

x|y	Keywords and parameters separated by a bar require you to choose one option.
x||y	Keywords and parameters separated by a double bar allows you to choose any or all of the options.

Information Icons

This book uses the following information symbols:

NOTE: The Note icon signals important operational information.

CAUTION: The Caution icon signals information about situations that could result in equipment damage or loss of data.

WARNING: The Warning icon signals information about hardware handling that could result in injury.

2

CLI Basics

This chapter describes the command line interface (CLI) structure and command modes. The Dell Networking operating system (FTOS) commands are in a text-based interface that allows you to use the launch commands, change command modes, and configure interfaces and protocols.

Accessing the Command Line

When the system boots successfully, you are positioned on the command line in EXEC mode and not prompted to log in. You can access the commands through a serial console port or a Telnet session. When you Telnet into the switch, you are prompted to enter a login name and password.

Example

```
telnet 172.31.1.53
Trying 172.31.1.53...
Connected to 172.31.1.53.
Escape character is '^]'.
Login: username
Password: FTOS>
```

After you log in to the switch, the prompt provides you with the current command-level information. For example:

Prompt	CLI Command Mode
`FTOS>`	EXEC
`FTOS#`	EXEC Privilege
`FTOS(conf)#`	CONFIGURATION

NOTE: For a list of all the command mode prompts, refer to the Command Modes section.

Multiple Configuration Users

When a user enters CONFIGURATION mode and another user is already in CONFIGURATION mode, FTOS generates an alert warning message similar to the following:

```
FTOS#conf

% Warning: The following users are currently configuring the system:

User "" on line console0
User "admin" on line vty0 ( 123.12.1.123 )
User "admin" on line vty1 ( 123.12.1.123 )
User "Irene" on line vty3 ( 123.12.1.321 )
FTOS#conf
```

When another user enters CONFIGURATION mode, FTOS sends a message similar to the following:

```
% Warning: User "admin" on line vty2 "172.16.1.210" is in configuration
```

In this case, the user is “admin” on vty2.

Navigating the CLI

FTOS displays a CLI prompt comprised of the host name and CLI mode.

- Host name is the initial part of the prompt and is “FTOS” by default. You can change the host name with the `hostname` command.
- CLI mode is the second part of the prompt and reflects the current CLI mode. For a list of the FTOS command modes, refer to the command mode list in the Accessing the Command Line section.

The CLI prompt changes as you move up and down the levels of the command structure. Starting with CONFIGURATION mode, the command prompt adds modifiers to further identify the mode. For more information about command modes, refer to the Command Modes section.

Obtaining Help

As soon as you are in a command mode there are several ways to access help.

To obtain a list of keywords at any command mode:	Type a `?` at the prompt or after a keyword. There must always be a space before the `?`.
To obtain a list of keywords with a brief functional description:	Type `help` at the prompt.
To obtain a list of available options:	Type a keyword and then type a space and a `?`.
To obtain a list of partial keywords using a partial keyword:	Type a partial keyword and then type a `?`.

Example

The following is an example of typing `ip ?` at the prompt:

```
FTOS(conf)#ip ?
access-list                     Named access-list
as-path                         BGP autonomous system path
filter
community-list                  Add a community list entry
control-plane                   Control plane configuration
dhcp                            DHCP configuration commands
domain-list                     Domain name to complete
unqualified host name
domain-lookup                   Enable IP Domain Name System
hostname translation
domain-name                     Define the default domain name
ecmp-group                      ECMP Group Configuration
```

```
extcommunity-list               Add a Extended community list
entry
ftp                             FTP configuration commands
helper-address                  DHCP relay agent configuration
host                            Add an entry to the ip
hostname table
igmp                            Internet Group Management
Protocol
max-frag-count                  Max. fragmented packets
allowed in IP re-assembly
mroute                          Multicast routes and counters
msdp                            Multicast source discovery
protocol
multicast-limit                 Max entries in Multicast TIB
multicast-msdp                  Enable IP multicast MSDP
protocol
multicast-routing               Enable IP multicast forwarding
name-server                     Specify addess of name server
to use
pim                             Protocol Independent Multicast
prefix-list                     Build a prefix list
radius                          Interface configuration for
RADIUS
route                           Establish static routes
scp                             SCP configuration commands
source-route                    Process packets with source
routing header options
ssh                             SSH configuration commands
tacacs                          Interface configuration for
TACACS+
telnet                          Specify telnet options
tftp                            TFTP configuration commands
FTOS(conf)#
```

When entering commands, you can take advantage of the following timesaving features:

- The commands are not case-sensitive.
- You can enter partial (truncated) command keywords. For example, you can enter `int te` followed by slot/port information for the `interface tengigabitethernet` command.
- Use the TAB key to complete keywords in commands.
- Use the up Arrow key to display the last enabled command.
- Use either the Backspace key or Delete key to erase the previous character.
- Use the left and right Arrow keys to navigate left or right in the FTOS command line.

The shortcut key combinations at the FTOS command line are as follows:

Key Combination	Action
CNTL-A	Moves the cursor to the beginning of the command line.
CNTL-B	Moves the cursor back one character.
CNTL-D	Deletes the character at the cursor.
CNTL-E	Moves the cursor to the end of the line.
CNTL-F	Moves the cursor forward one character.
CNTL-I	Completes a keyword.

Key Combination	Action
CNTL-K	Deletes all the characters from the cursor to the end of the command line.
CNTL-L	Re-enters the previous command.
CNTL-N	Returns to the more recent commands in the history buffer after recalling commands with Ctrl-P or the up Arrow key.
CNTL-P	Recalls commands, beginning with the last command.
CNTL-R	Re-enters the previous command.
CNTL-U	Deletes the line.
CNTL-W	Deletes the previous word.
CNTL-X	Deletes the line.
CNTL-Z	Ends continuous scrolling of the command outputs.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Esc D	Deletes all the characters from the cursor to the end of the word.

Using the Keyword no Command

To disable, delete or return to default values, use the `no` form of the commands.

For most commands, if you type the keyword `no` in front of the command, you disable that command or delete it from the running configuration. In this guide, the `no` form of the command is described in the Syntax portion of the command description.

Filtering show Commands

To find specific information, display certain information only or begin the command output at the first instance of a regular expression or phrase, you can filter the display output of a `show` command.

When you execute a `show` command, and then enter a pipe (|), one of the parameters listed below, and a regular expression, the resulting output either excludes or includes those parameters.

NOTE: FTOS accepts a space before or after the pipe, no space before or after the pipe, or any combination. For example: `FTOS#command | grep gigabit |except regular-expression | find regular-expression`

`display`	displays additional configuration information
`except`	displays only the text that does not match the pattern (or regular expression)
`find`	searches for the first occurrence of a pattern
`grep`	displays text that matches a pattern.

The `grep` command option has an ignore-case suboption that makes the search case-insensitive. For example, the commands:

**`show run	grep Ethernet`**	returns a search result with instances containing a capitalized “Ethernet,” such as `interface GigabitEthernet 0/0`
**`show run	grep ethernet`**	does not return the above search result because it only searches for instances containing a noncapitalized “ethernet”
**`show run	grep Ethernet ignore-case`**	returns instances containing both “Ethernet” and “ethernet”

`no-more`	does not paginate the display output
`save`	copies the output to a file for future use

Displaying All Output

To display the output all at once (not one screen at a time), use the `no-more` option after the pipe. This operation is similar to the `terminal length screen-length` command except that the `no-more` option affects the output of just the specified command. For example: `FTOS#show running-config|no-more`.

Filtering the Command Output Multiple Times

You can filter a single command output multiple times. To filter a command output multiple times, place the `save` option as the last filter. For example: `FTOS# command | grep regular-expression | except regular-expression | grep other-regular-expression | find regular-expression | no-more | save`.

Command Modes

To navigate and launch various CLI modes, use specific commands. Navigation to these modes is described in the following sections.

NOTE: Some of the following modes are not available on the S5000.

EXEC Mode

When you initially log in to the switch, by default, you are logged in to EXEC mode. This mode allows you to view settings and enter EXEC Privilege mode, which is used to configure the device.

When you are in EXEC mode, the > prompt is displayed following the host name prompt, which is “FTOS” by default. You can change the host name prompt using the `hostname` command.

NOTE: Each mode prompt is preceded by the host name.

EXEC Privilege Mode

The `enable` command accesses EXEC Privilege mode. If an administrator has configured an “Enable” password, you are prompted to enter it.

EXEC Privilege mode allows you to access all the commands accessible in EXEC mode, plus other commands, such as to clear address resolution protocol (ARP) entries and IP addresses. In addition, you can access CONFIGURATION mode to configure interfaces, routes and protocols on the switch. While you are logged in to EXEC Privilege mode, the # prompt is displayed.

CONFIGURATION Mode

In EXEC Privilege mode, use the `configure` command to enter CONFIGURATION mode and configure routing protocols and access interfaces.

To enter CONFIGURATION mode:

1. Verify that you are logged in to EXEC Privilege mode.
2. Enter the `configure` command. The prompt changes to include (conf).

From this mode, you can enter INTERFACE mode by using the `interface` command.

INTERFACE Mode

You must use INTERFACE mode to configure interfaces or IP services on those interfaces. An interface can be physical (for example, a Ten-Gigabit Ethernet port) or virtual (for example, the Null interface).

To enter INTERFACE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `interface` command with an interface type and slot/port numbers.

The prompt changes, as listed below, to include the designated interface and slot/port numbers.

NOTE: On the S5000, the valid *slot* numbers are the supported stack-unit numbers (0 to 11). The valid *port* numbers for each interface type are listed below.

Prompt	Interface Type
`FTOS(conf-if)#`	INTERFACE mode
`FTOS(conf-if-gi-0/0)#`	`gigabitethernet` followed by the slot/port information (ports 0–47)
`FTOS(conf-if-te-0/0)#`	`tengigabitethernet` followed by slot/port information (ports 0–63)
`FTOS(conf-if-fo-0/0)#`	`fortyGigE`followed by slot/port information (ports 48, 52, 56, or 60)
`FTOS(conf-if-fc-0/0)#`	`FibreChannel` followed by slot/port information (ports 0–47)
`FTOS(conf-if-lo-0)#`	`loopback` followed by a number (range 0–16383)
`FTOS(conf-if-nu-0)#`	`null` followed by zero (0)

Prompt	Interface Type
`FTOS(conf-if-po-0)#`	`port-channel` number (range 1–128)
`FTOS(conf-if-vl-0)#`	`vlan` followed by VLAN id number (range 1–4094)
`FTOS(conf-if-ma-0/0)#`	`managementethernet` followed by slot/port information (port 0)
`FTOS(conf-if-range)#`	Designated interface range (used for bulk configuration).

LINE Mode

You must use LINE mode to configure the console or virtual terminal parameters.

To enter LINE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `line` command. Include the keywords `console` or `vty` and their line number available on the switch. The prompt changes to include (config-line-console) or (config-line-vty).

You can exit this mode by using the `exit` command.

TRACE-LIST Mode

You must use TRACE-LIST mode to configure a Trace list.

To enter TRACE-LIST mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `ip trace-list` command. Include the name of the Trace list. The prompt changes to include (conf-trace-acl).

You can exit this mode by using the `exit` command.

MAC ACCESS LIST Mode

You must use the `mac access-list standard` or `mac access-list extended` command to enter MAC ACCESS LIST mode and configure either standard or extended access control lists (ACLs).

To enter MAC ACCESS LIST mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Use the `mac access-list standard` or `mac access-list extended` command. Include a name for the ACL. The prompt changes to include (conf-std-macl) or (conf-ext-macl).

You can return to CONFIGURATION mode by using the `exit` command.

IP ACCESS LIST Mode

You must use the `ip access-list standard` or `ip access-list extended` command to enter IP ACCESS LIST mode and configure either standard or extended access control lists (ACLs).

To enter IP ACCESS LIST mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Use the `ip access-list standard` or `ip access-list extended` command. Include a name for the ACL. The prompt changes to include (conf-std-nacl) or (conf-ext-nacl).

You can return to CONFIGURATION mode by using the `exit` command.

ROUTE-MAP Mode

You must use ROUTE-MAP mode to configure a route map.

To enter ROUTE-MAP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Use the `route-map` *map-name* `[permit | deny] [`*sequence-number*`]` command. The prompt changes to include (route-map).

You can return to CONFIGURATION mode by using the `exit` command.

PREFIX-LIST Mode

You must use PREFIX-LIST mode to configure a prefix list.

To enter PREFIX-LIST mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `ip prefix-list` command. Include a name for the prefix list. The prompt changes to include (conf-nprefixl).

You can return to CONFIGURATION mode by using the `exit` command.

AS-PATH ACL Mode

You must use AS-PATH ACL mode to configure an AS-PATH Access Control List (ACL) on the S5000. For more information, refer to Access Control Lists (ACL).

To enter AS-PATH ACL mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `ip as-path access-list` command. Include a name for the AS-PATH ACL. The prompt changes to include (config-as-path).

You can return to CONFIGURATION mode by using the `exit` command.

IP COMMUNITY LIST Mode

You must use IP COMMUNITY LIST mode to configure an IP Community ACL on the S5000. For more information, refer to Access Control Lists (ACL).

To enter IP COMMUNITY LIST mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `ip community-list` command. Include a name for the Community list. The prompt changes to include (config-community-list).

You can return to CONFIGURATION mode by using the `exit` command.

REDIRECT-LIST Mode

You must use REDIRECT-LIST mode to configure a Redirect list on the S5000. For more information, refer to the *S5000 FTOS Command Line Reference Guide*, Policy-based Routing (PBR).

To enter REDIRECT-LIST mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Use the `ip redirect-list` command. Include a name for the Redirect-list. The prompt changes to include (conf-redirect-list).

You can return to CONFIGURATION mode by using the `exit` command.

SPANNING TREE Mode

You must use SPANNING TREE mode to enable and configure the Spanning Tree protocol. For more information, refer to Spanning Tree Protocol (STP).

To enter SPANNING TREE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol spanning-tree` *stp-id* command.

You can return to CONFIGURATION mode by using the `exit` command

Per-VLAN SPANNING TREE (PVST+) Plus Mode

You must use PVST+ mode to enable and configure the Per-VLAN Spanning Tree (PVST+) protocol. For more information, refer to Per-VLAN Spanning Tree Plus (PVST+).

NOTE: The protocol name is PVST+, but the plus sign is dropped at the CLI prompt.

To enter PVST+ mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol spanning-tree pvst` command.

You can return to CONFIGURATION mode by using the `exit` command.

RAPID SPANNING TREE (RSTP) Mode

You must use RSTP mode to enable and configure RSTP. For more information, refer to Rapid Spanning Tree Protocol (RSTP).

To enter RSTP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol spanning-tree rstp` command.

You can return to CONFIGURATION mode by using the `exit` command.

MULTIPLE SPANNING TREE (MSTP) Mode

You must use MULTIPLE SPANNING TREE mode to enable and configure MSTP. For more information, refer to Multiple Spanning Tree Protocol (MSTP).

To enter MULTIPLE SPANNING TREE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol spanning-tree mstp` command.

You can return to CONFIGURATION mode by using the `exit` command.

PROTOCOL GVRP Mode

You must use PROTOCOL GVRP mode to enable and configure GARP VLAN Registration Protocol (GVRP). For more information, refer to GARP VLAN Registration (GVRP).

To enter PROTOCOL GVRP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol gvrp` command.

You can return to CONFIGURATION mode by using the `exit` command.

ROUTER OSPF Mode

You must use ROUTER OSPF mode to configure OSPF. For more information, refer to Open Shortest Path First (OSPFv2).

To enter ROUTER OSPF mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `router ospf {process-id}` command. The prompt changes to include (conf-router_ospf-id).

You can switch to INTERFACE mode by using the `interface` command or you can switch to ROUTER RIP mode by using the `router rip` command.

ROUTER RIP Mode

You must use ROUTER RIP mode to configure RIP on the S5000. For more information, refer to Routing Information Protocol (RIP).

To enter ROUTER RIP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `router rip` command. The prompt changes to include (conf-router_rip).

You can switch to INTERFACE mode by using the `interface` command or you can switch to ROUTER OSPF mode by using the `router ospf` command.

ROUTER ISIS Mode

You must use ROUTER ISIS mode to configure intermediate system to intermediate system (ISIS) on the S5000. For more information, refer to the Intermediate System to Intermediate System (IS-IS) chapter in the *S5000 FTOS Command Line Reference Guide*.

To enter ROUTER ISIS mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `router isis [tag]` command. The prompt changes to include (conf-router_isis).

You can switch to INTERFACE mode by using the `interface` command or you can switch to ROUTER RIP mode by using the `router rip` command.

ROUTER BGP Mode

You must use ROUTER BGP mode to configure Border Gateway Protocol (BGP) on the S5000. For more information, refer to Border Gateway Protocol IPv4 (BGPv4).

To enter ROUTER BGP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `router bgp` *`as-number`* command. The prompt changes to include (conf-router_bgp).

You can return to CONFIGURATION mode by using the `exit` command.

VLT DOMAIN Mode

Use VLT DOMAIN mode to enable and configure the VLT domain protocol. For more information, refer to Virtual Link Trunking (VLT).

To enter VLT DOMAIN mode:

1. Verify that you are logged into CONFIGURATION mode.
2. Enter the `config-vlt-domain` command.

You can return to CONFIGURATION mode by entering the `exit` command.

Determining Chassis Mode

Chassis mode in FTOS determines which hardware is being supported in an S5000 switch.

Chassis mode is programmed into an electrically erasable programmable read-only memory (EEPROM) on the backplane of the chassis and the change takes place only after the chassis is rebooted. Configuring the appropriate chassis mode allows the system to use all the available ports and to recognize all software features.

3

File Management

This chapter contains command line interface (CLI) commands needed to manage the configuration files as well as other file management commands.

The commands in this chapter are supported by the Dell Networking operating system (FTOS) on the S5000 platform.

cd

Change to a different working directory.

S5000

Syntax	`cd` *`directory`*
Parameters	*directory* (OPTIONAL) Enter `flash:` (internal Flash) or any sub-directory.
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

copy

Copy one file to another location. FTOS supports IPv4 and IPv6 addressing for FTP, TFTP, and SCP (in the *hostip* field).

S5000

Syntax `copy` *`source-file-url destination-file-url`*

Parameters Enter the following location keywords and information:

file-url	**To copy a file from the internal FLASH**	enter `flash://` followed by the filename
	To copy a file on an FTP server	enter `ftp://` *`user:password@hostip/filepath`*

To copy the running configuration	enter the keyword `running-config`
To copy the startup configuration	enter the keyword `startup-config`
To copy using a Secure Copy (SCP),	enter the keyword `scp:` • If you enter `scp:` in the source position, enter the target URL; • If you enter `scp:` in the target position, first enter the source URL;
To copy a file on the external FLASH	enter `usbflash://` followed by the filename
To copy a file on a TFTP server	enter `tftp://`*`hostip/filepath`*

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

FTOS supports a maximum of 100 files at the root directory level, on both the internal and external Flash.

When copying a file to a remote location (for example, using Secure Copy [SCP]), enter only the keywords and FTOS prompts you need for the rest of the information. For example, when using SCP, you can enter `copy running-config scp:` where `running-config` is the source and the target is specified in the ensuing prompts. FTOS prompts you to enter any required information, as needed for the named destination—remote destination, destination filename, user ID, password, etc.

When you use the `copy running-config startup-config` command to copy the running configuration (the startup configuration file amended by any configuration changes made since the system was started) to the startup configuration file, FTOS creates a backup file on the internal flash of the startup configuration.

FTOS supports copying the running-configuration to a TFTP server or to an FTP server. For example:

- `copy running-config tftp:`
- `copy running-config ftp:`

Example

```
FTOS#copy running-config scp:/
Address or name of remote host []: 10.10.10.1
Destination file name [startup-config]? old_running
User name to login remote host? sburgess
Password to login remote host? dilling
```

In this `copy scp: flash:` example, specifying `SCP` in the first position indicates that the target is to be specified in the ensuing prompts. Entering `flash:` in the second position indicates that the target is the internal Flash. The source is on a secure server running SSH, so you are prompted for the user datagram protocol (UDP) port of the SSH server on the remote host.

Example

```
FTOS#copy scp: flash:
Address or name of remote host []: 10.11.199.134
Port number of the server [22]: 99
Source file name []: test.cfg
User name to login remote host: admin
Password to login remote host:
Destination file name [test.cfg]: test1.cfg
```

Related Commands

cd – changes the working directory.

copy running-config startup-config

Copy running configuration to the startup configuration.

S5000

Syntax `copy running-config startup-config {duplicate}`

Command Modes EXEC Privilege

Command History

Version 9.0.(1.3)	Introduced on the S5000.

Usage Information

This command is useful for quickly making a changed configuration on one chassis available on external flash in order to move it to another chassis.

When you use the `copy running-config startup-config duplicate` command to copy the running configuration to the startup configuration, FTOS creates a backup file on the internal flash of the startup configuration.

delete

Delete a file from the flash. After deleted, files cannot be restored.

S5000

Syntax `delete flash-url [no-confirm]`

Parameters

flash-url	Enter the following location and keywords: • For a file or directory on the internal Flash, enter `flash://` followed by the filename or directory name. • For a file or directory on the external Flash, enter `slot0://` followed by the filename or directory name.

	no-confirm	(OPTIONAL) Enter the keyword `no-confirm` to specify that FTOS does not require user input for each file prior to deletion.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

dir

Display the files in a file system. The default is the current directory.

S5000

Syntax `dir [filename | directory name:]`

Parameters

filename | directory name:	(OPTIONAL) Enter one of the following: • For a file or directory on the internal Flash, enter `flash://` followed by the filename or directory name. • For a file or directory on the external Flash, enter `slot0://` followed by the filename or directory name.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#dir
Directory of flash:
1 -rwx 6478482 May 13 101 16:54:34 E1200.BIN
flash: 64077824 bytes total (57454592 bytes free)
FTOS#
```

Related Commands cd – changes the working directory.

format flash

Erase all existing files and reformat the filesystem in the internal flash memory. After the filesystem is formatted, files cannot be restored.

S5000

Syntax `format flash:`

Defaults

flash memory

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must include the colon (:) when entering this command.

After reformatting is complete, three empty directories are automatically created on flash: CRASH_LOG_DIR, TRACE_LOG_DIR and NVTRACE_LOG_DIR.

CAUTION: This command deletes all files, including the startup configuration file. So, after executing this command, consider saving the running config as the startup config (use the `write memory` command or `copy run start` command).

Related Commands

copy – copies the current configuration to either the startup-configuration file or the terminal.

show file – displays the contents of a text file in the local filesystem.

show file-systems – displays information about the file systems on the system.

format usbflash

Erase all existing files and reformat the file system in USB flash memory. After the file system is formatted, files cannot be restored.

S5000

Syntax

`format usbflash://`

Defaults

None

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must include the colon and two forward slashes (://) when entering this command.

CAUTION: This command deletes all files in the USB flash memory. After you insert an external flash device into the USB port on an S5000 and enter the format usbflash:// command to erase all existing files and reformat the file system on the device, you must allow the process to run to completion before removing it from the USB port. If you remove the USB flash device before the formatting is complete, you must reload the S5000 before you can try formatting the device again.

Related Commands

copy – copies the current configuration to either the startup-configuration file or the terminal.

logging coredump

Enable coredump.

S5000

Syntax

```
logging coredump {stack-unit all}
```

Parameters

stack-unit all	Enable coredump on all stack-units.

Defaults The kernal coredump is disabled.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The kernel coredump can be large and may take five to 30 minutes to upload.

FTOS does not overwrite application coredumps so you should delete them as necessary to conserve space on the flash; if the flash is out of memory, the coredump is aborted.

On the S5000, if the FTP server is not reachable, the application coredump is aborted. FTOS completes the coredump process and waits until the upload is complete before rebooting the system.

Related Commands

logging coredump server – designates a sever to upload kernel coredumps.

logging coredump server

Designate a server to upload core dumps.

S5000

Syntax

```
logging coredump server {ipv4-address | ipv6-address} username
name password [type] password
```

Parameters

{ipv4-address | ipv6-address}	Enter the server IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X).
name	Enter a username to access the target server.
type	Enter the password type: • Enter `0` to enter an unencrypted password. • Enter `7` to enter a password that has already been encrypted using a Type 7 hashing algorithm.
password	Enter a password to access the target server.

Defaults	Crash kernel files are uploaded to flash by default.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Because flash space may be limited, using this command ensures your entire crash kernel files are uploaded successfully and completely. Only a single coredump server can be configured. Configuration of a new coredump server over-writes any previously configured server. **NOTE:** You must disable logging coredump before you designate a new server destination for your core dumps.
Related Commands	logging coredump – disables the kernel coredump

pwd

Display the current working directory.

S5000

Syntax	`pwd`
Defaults	Crash kernel files are uploaded to flash by default.
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
FTOS#pwd
flash:
FTOS#
```

Related Commands	cd – changes the directory.

rename

Rename a file in the local file system.

S5000

Syntax	`rename` *`url url`*

Parameters		
	url	Enter the following keywords and a filename: • For a file on the internal Flash, enter `flash://` followed by the filename. • For a file on the external Flash, enter `slot0://` followed by the filename.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show file

Display contents of a text file in the local filesystem.

S5000

Syntax `show file filesystem`

Parameters		
	filesystem	Enter one of the following: • For internal flash, enter `flash:` • For external Flash, enter `slot0:`

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show file flash://startup-config
! Version S5000-SYS-9-0-1-2
! Last configuration change Thu Nov 1 00:06:24 2012 by default
! Startup-config last updated Thu Nov 1 00:06:31 2012 by
default
!
boot system stack-unit 0 primary tftp://10.10.1.12/pt-s5000-3
boot system gateway 192.168.1.1
!
redundancy auto-synchronize full
redundancy disable-auto-reboot stack-unit
!
redundancy disable-auto-reboot stack-unit 0
...
redundancy disable-auto-reboot stack-unit 11
!
logging coredump stack-unit all
!
hostname s5000-4
!
enable password 7 b125455cf679b208e79b910e85789edf
```

```
!
username admin password 7 1d28e9f33f99cf5c
!
stack-unit 0 provision S5000
!
interface TenGigabitEthernet 0/0
 no ip address
 no shutdown
...
interface fortyGigE 0/48
 no ip address
 no shutdown
...
interface fortyGigE 0/60
 no ip address
 no shutdown
!
interface ManagementEthernet 0/0
 ip address 10.1.1.1/16
 no shutdown
...
interface Vlan 1
!
snmp-server community public ro
!
protocol lldp
!
line console 0
line vty 0
line vty 1
...
!
end
FTOS#
```

Related Commands

format flash – Erases all the existing files and reformats the filesystem in the internal flash memory on the S5000.

show file-systems – displays information about the file systems on the system.

show file-systems

Display information about the file systems on the system.

S5000

Syntax

`show file-systems`

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show file-systems

   Size(b)     Free(b) Feature      Type Flags  Prefixes
2143281152 2143227904   FAT32 USERFLASH    rw   flash:
```

```
              -            -         -    network     rw   ftp:
              -            -         -    network     rw   tftp:
              -            -         -    network     rw   scp:
FTOS#
```

Usage Information

Field	Description
size(b)	Lists the size (in bytes) of the storage location. If the location is remote, no size is listed.
Free(b)	Lists the available size (in bytes) of the storage location. If the location is remote, no size is listed.
Feature	Displays the formatted DOS version of the device.
Type	Displays the type of storage. If the location is remote, the word `network` is listed.
Flags	Displays the access available to the storage location. The following letters indicate the level of access: • r = read access • w = write access
Prefixes	Displays the name of the storage location.

Related Commands

format flash – Erases all the existing files and reformats the filesystem in the internal flash memory on the S5000.

show file – Displays the contents of a text file in the local filesystem.

show os-version

Display the release and software image version information of the image file specified.

S5000

Syntax `show os-version [file-url]`

Parameters

file-url	(OPTIONAL) Enter the following location keywords and information: • For a file on the internal flash, enter `flash://` followed by the filename. • For a file on an FTP server, enter `ftp://user:password@hostip/filepath`. • For a file on the external Flash, enter `slot0://` followed by the filename. • For a file on a TFTP server, enter `tftp://hostip/filepath`.

NOTE: `ftp` and `tftp` are the only S5000 options.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

NOTE: A filepath that contains a dot (.) is not supported.

Example

```
FTOS#  show os-version

RELEASE IMAGE INFORMATION :
---------------------------------------------------------------
------
      Platform          Version        Size
ReleaseTime
S-Series:  SH        9.0(1.3)    61061147    May  9 2013
20:02:52

TARGET IMAGE INFORMATION :
---------------------------------------------------------------
------
          Type          Version                   Target
checksum
       runtime        9.0(1.3)        Control Processor
passed
       runtime        9.0(1.3)                  fcimage
passed

BOOT IMAGE INFORMATION :
---------------------------------------------------------------
------
          Type          Version                   Target
checksum
    boot flash          1.3.1.0        Control Processor
passed

BOOTSEL IMAGE INFORMATION :
---------------------------------------------------------------
------
          Type          Version                   Target
checksum
boot selector          1.3.0.1        Control Processor
passed

CPLD IMAGE INFORMATION :
---------------------------------------------------------------
------
         Card                      CPLD Name    Version
Stack-unit 0             S5000 SYSTEM CPLD         41
FTOS#
```

show running-config

Display the current configuration and display changes from the default values.

S5000

Syntax `show running-config [entity] [configured] [status]`

Parameters

entity (OPTIONAL) Enter one of the keywords listed below to display that entity's current (non-default) configuration:

NOTE: If nothing is configured for that entity, nothing is displayed and the prompt returns.

aaa	for the current AAA configuration
acl	for the current ACL configuration
arp	for the current static ARP configuration
as-path	for the current AS-path configuration
bfd	for the current BFD configuration
bgp	for the current BGP configuration
boot	for the current boot configuration
cam-profile	for the current CAM profile in the configuration
class-map	for the current class-map configuration
community-list	for the current community-list configuration
ecmp-group	for the current ECMP group configuration
ethernet	for the current Ethernet CFM configuration
fefd	for the current FEFD configuration
ftp	for the current FTP configuration
frrp	for the current FRRP configuration
fvrp	for the current FVRP configuration
gvrp	for the current GVRP configuration
host	for the current host configuration
hardware-monitor	for hardware-monitor action-on-error settings
hypervisor	for the current hypervisor configuration
igmp	for the current IGMP configuration
interface	for the current interface configuration
ip	for the current IP configuration

isis	for the current ISIS configuration
line	for the current line configuration
lldp	for the current LLDP configuration
load-balance	for the current port-channel load-balance configuration
logging	for the current logging configuration
mac	for the current MAC ACL configuration
mac-address-table	for the current MAC configuration
management-route	for the current Management port forwarding configuration
mld	for the current MLD configuration
monitor	for the current Monitor configuration
mroute	for the current Mroutes configuration
msdp	for the current MSDP configuration
ntp	for the current NTP configuration
ospf	for the current OSPF configuration
pim	for the current PIM configuration
policy-map-input	for the current input policy map configuration
policy-map-output	for the current output policy map configuration
po-failover-group	for the current Port-channel failover-group configuration
prefix-list	for the current prefix-list configuration
privilege	for the current privilege configuration
qos-policy-input	for the current input qos policy configuration
qos-policy-output	for the current output qos policy configuration
radius	for the current RADIUS configuration
redirect-list	for the current redirect-list configuration
redundancy	for the current stack-unit redundancy configuration
resolve	for the current DNS configuration
rip	for the current RIP configuration

rmon	for the current RMON configuration
route-map	for the current route map configuration
sflow	for the current sFlow configuration
snmp	for the current SNMP configuration
spanning-tree	for the current spanning tree configuration
static	for the current static route configuration
status	for the file status information
tacacs+	for the current TACACS+ configuration
tftp	for the current TFTP configuration
trace-group	for the current trace-group configuration
trace-list	for the current trace-list configuration
uplink-state-group	for the uplink state group configuration
users	for the current users configuration
vlt	for the current VLT configuration
wred-profile	for the current wred-profile configuration

configured	(OPTIONAL) Enter the keyword `configuration` to display switch interfaces with non-default configurations only.
status	(OPTIONAL) Enter the keyword `status` to display the checksum for the running configuration and the start-up configuration.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show running-config
Current Configuration ...
! Version 9-0(1-2)
! Last configuration change at Mon Jun 10 21:20:04 2030 by
admin
!
boot system stack-unit 0 primary system: B:
boot system stack-unit 0 secondary tftp://10.200.200.241/kp-
diablo
boot system stack-unit 0 default tftp://10.11.200.241/kp-diablo
!
redundancy auto-synchronize full
!
service timestamps log datetime
!
hostname FTOS
!
enable password 7 b125455cf679b208e79b910e85789edf
!
username admin password 7 1d28e9f33f99cf5c
```

```
!
stack-unit 0 provision S5000
!
interface fibrechannel 0/0
shutdown
!
interface fibrechannel 0/1
shutdown
!
interface TenGigabitEthernet 0/0
no ip address
shutdown
!
interface TenGigabitEthernet 0/1
no ip address
shutdown
!
....
interface TenGigabitEthernet 0/35
no ip address
shutdown
!
interface fortyGigE 0/48
no ip address
shutdown
!
interface fortyGigE 0/52
no ip address
shutdown
!
interface fortyGigE 0/56
no ip address
shutdown
!
interface fortyGigE 0/60
no ip address
shutdown
!
interface ManagementEthernet 0/0
ip address 10.1.1.1/16
no shutdown
!
....
!
interface ManagementEthernet 11/0
no shutdown
!
interface Vlan 1
!
service-class dynamic dot1p
!
snmp-server community public ro
!
protocol lldp
!
line console 0
line vty 0
....
line vty 9
!
end
FTOS#

FTOS#show running-config status
```

```
running-config bytes 4419, checksum 0x8A1D926E
startup-config bytes 3002, checksum 0xAFFD4BCA
FTOS#
```

Example

```
FTOS#show running-config status
running-config bytes 3956, checksum 0xD236FC8A
startup-config bytes 3905, checksum 0xE0F391F8
FTOS#
```

Usage Information

The `status` option allows you to display the size and checksum of the running configuration and the startup configuration.

show stack-unit

View the current stack-unit status.

S5000

Syntax `show stack-unit [unit-id | all]`

Parameters

stack-unit ***unit-id***	Enter the number of a stack-unit to view information on that stack-unit. The range is 0 to 11.
all	(OPTIONAL) Enter the keyword `all` to view a table with information on all present stack-units.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (needed)

```
FTOS#show stack-unit 0


FTOS#
```

show startup-config

Display the startup configuration.

S5000

Syntax `show startup-config`

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show startup-config
! Version 9-0(1-2)
! Last configuration change at Mon Jun 10 19:20:41 2030 by
default
! Startup-config last updated at Mon Jun 10 19:20:42 2030 by
default
!
boot system stack-unit 0 primary system: B:
boot system stack-unit 0 secondary tftp://10.200.200.241/kp-
diablo
boot system stack-unit 0 default tftp://10.11.200.241/kp-diablo
!
redundancy auto-synchronize full redundancy disable-auto-
reboot stack-unit
!
!------------------ output truncated -------------------!
FTOS#
```

Related Commands

show running-config – displays the current (running) configuration.

show version

Display the current FTOS version information on the system.

S5000

Syntax `show version`

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Field	**Description**
Dell Force10 Real Time...	Name of the operating system
Dell Force10 Operating...	OS version number
Dell Force10 Application	Software version
Fiber Channel Firmware...	Fibre Channel firmware version
Copyright (c)...	Copyright information
Build Time...	Software build's date stamp

Build Path...	Location of the software build files loaded on the system
FTOS uptime is...	Amount of time the system has been up
System image...	Image file name
System Type...	Switch type (S5000)
Control Processor...	Control processor information and amount of memory on processor
16M bytes...	Amount and type of memory on system
1 4–module...24 Ten GigabitEthernet... Forty GigabitEthernet...	Hardware configuration of the system, including the number and type of physical interfaces available

Example

```
FTOS#show version
Dell Force10 Real Time Operating System Software
Dell Force10 Operating System Version: 2.0
Dell Force10 Application Software Version: 9.0(1.3)
Fiber Channel Firmware Version: V10.1.0.00.04
Copyright (c) 1999-2013 by Dell Inc. All Rights Reserved.
Build Time: Sun Apr 21 23:46:40 PDT 2013
Build Path: /sites/sjc/work/build/buildSpaces/build02/
E9-0-1/SW/SRC
FTOS uptime is 2 week(s), 5 day(s), 0 hour(s), 54 minute(s)

System image file is "system://A"

System Type: S5000
Control Processor: Freescale QorIQ P2020 with 2147483648 bytes
of memory.

16M bytes of boot flash memory.

  5 4-module, 4-port GE/TE/FG (SH)
84 Ten GigabitEthernet/IEEE 802.3 interface(s)
20 Forty GigabitEthernet/IEEE 802.3 interface(s)
FTOS#
```

upgrade boot (standalone unit)

Upgrade the bootflash or bootselector image on a standalone S5000 switch.

S5000

Syntax

`upgrade boot {bootflash-image| bootselector-image} stack-unit` *`stack-unit—id`* `{booted: | flash://`*`file-path`* `| ftp://`*`file-path`* `| tftp://`*`file-path`* `| usbflash://`*`file-path`*`}`

Parameters

boot	Enter the keyword `boot` to change the boot image.

bootflash-image	Upgrade the boot image in the bootflash partition.
bootselector-image	Upgrade the boot image in the bootselector partition. You are prompted to enter the password.
stack-unit ***stack-unit-id***	Enter the keyword `stack-unit` followed by the stack unit ID of the switch. Valid values are from 0 to 11.
booted:	Upgrade using the boot image with which the S5000 booted up.
flash:	After the keyword `flash:`, enter the location of the source file in the internal flash in the format: `flash://`*`filepath`* or press **Enter** to launch a prompt sequence.
ftp:	After the keyword `ftp:`, enter the location of the source file in the format: `//`*`userid`*`:`*`password`*`@`*`host-ip`*`/`*`file-path`* or press **Enter** to launch a prompt sequence.
tftp:	After the keyword `tftp:`, enter the location of the source file in the format: `//`*`host-path`*`/`*`file-path`* or press **Enter** to launch a prompt sequence.
usbflash:	After the keyword `usbflash:`, enter the location of the source file in the external flash in the format: `usbflash://`*`filepath`* or press **Enter** to launch a prompt sequence.
file-path	Enter the path and filename to be used to upgrade the boot image.

Defaults None

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information You must reload the switch after entering the `upgrade boot` command to boot up the switch with the new boot code.

Example

```
FTOS#upgrade  boot bootselector-image  stack-unit 0 booted

Password:

Current BootSelector information in the system:
===============================================

  Card                  BootSelector    Current Version
New Version
---------------------------------------------------------------
---------
Unit0                 Boot Selector
1.3.0.0         1.3.0.1


***************************************************************
********
```

```
    *  Warning - Upgrading boot selectors is inherently risky
and should  *
    *  only be attempted when necessary.  A failure at this
upgrade may   *
    *  cause a board RMA.  Proceed with
caution !                        *

***************************************************************
********

Proceed upgrade Boot Selector image for stack-unit 0 [yes/no]:
yes


Programming
!.!!.!.!.!!.!.!!.!.!!.!.!.!!.!.!.!!.!.!!.!.!.!!.!.!!.!.!.!!.!.!
!.!.!.!!.!.!.!.
Bootselector image upgrade for stack-unit 0 completed
successfully.


FTOS#upgrade  boot bootflash-image  stack-unit  0 booted

Current BootFlash information in the system:
===============================================

  Card                      BootFlash    Current Version
New Version
---------------------------------------------------------------
---------
Unit0                   Boot Flash B
1.3.1.1         1.3.1.2


***************************************************************
********
    *  Warning - Upgrading boot flash is inherently risky and
should only *
    *  be attempted when necessary.  A failure at this upgrade
may cause  *
    *  a board RMA.  Proceed with
caution !                              *

***************************************************************
*******

Proceed upgrade Boot Flash image for stack-unit 0 [yes/no]: yes


Programming
!!.!.!!.!.!!.!.!.!!.!.!!.!.!.!!.!.!.!!.!.!!.!.!.!!.!.!.!!.!.!!.
!.!!.!.!!.!.!.!!.!.!!.!.!!.!.!.!!.!.!!.!.!.!!.!May 14
19:23:21: %STKUNIT0-M:CP %SYSADM-5-CPU_THRESHOLD: Overall cpu
usage of management-unit is above threshold. Cpu1minUsage (88%)
May 14 19:23:21: %STKUNIT0-M:CP %SYSADM-5-TASK_CPU_THRESHOLD:
1min cpu utilization of management-unit has exceeded the
threshold. Top three processes are sysdlp (79.60%), system
(7.33%), sysd (1.11%)
.!!.!.!!.!.!.!!.!.!.!!.!.!!.!.!.!!.!.!!.!.!.!!.!.!!.!.!!.!.!.!.
!!.!.!!.!.!!.!.!.!!.!.!!.!.!.!!.!.!.!!.!.!!.!.!.!!.!.!!.!.!!.!.
!.!.!!.!.!!.!.!.!!.!.!.!!.!.!!.!.!!.!.!.!!.!.!!.!.!.!!.!.!!.!.!
!.!.!.!!.!.!.!!.!.!.!
```

```
Bootflash image upgrade for stack-unit 0 completed
successfully.
```

upgrade system (standalone unit)

Upgrade the FTOS image on a standalone S5000 switch.

S5000

Syntax `upgrade system {flash://`*`file-path`*` | ftp://`*`file-path`*` | scp://`*`file-path`*` | tftp://`*`file-path`*` | usbflash://`*`file-path`*`} {A: | B:}`

Parameters

system	Enter the keyword `system` to change the FTOS image.
flash:	After the keyword `flash:`, enter the location of the source file in the internal flash in the format: `//`*`file-path`* or press **Enter** to launch a prompt sequence.
ftp:	After the keyword `ftp:`, enter the location of the source file in the format: `//`*`userid`*`:`*`password`*`@`*`host-ipaddress`*`/`*`file-path`* or press **Enter** to launch a prompt sequence.
scp:	After the keyword `scp:`, enter the location of the source file in the format: `//`*`userid`*`:`*`password`*`@`*`host-ip-address`*`/`*`file-path`* or press **Enter** to launch a prompt sequence.
tftp:	After the keyword `tftp:`, enter the location of the source file in the format: `//`*`host-ip-address`*`/`*`file-path`* or press **Enter** to launch a prompt sequence.
usbflash:	After the keyword `usbflash:`, enter the location of the source file in the external flash in the format: `usbflash://`*`filepath`* or press **Enter** to launch a prompt sequence.
file-path	Enter the path and filename to be used to upgrade the FTOS image.
A:* | *B:	Enter the FTOS partition to be upgraded with the new image.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#upgrade system ?
flash: Copy from flash file system (flash://filepath)
ftp: Copy from remote file system, IPv4 or IPv6, (ftp://
userid:password@hostip/filepath)
scp: Copy from remote file system, IPv4 or IPv6, (scp://
userid:password@hostip/filepath)
stack-unit: Sync image to the stack-unit
tftp: Copy from remote file system, IPv4 or IPv6, (tftp://
hostip/filepath)
```

```
FTOS#upgrade  system  ftp:// A:
Address or name of remote host []: 10.11.200.241
Source file name []: /sw/Releases/FTOS-SH-9.0(1.3).bin
User name to login remote host: ftp
Password to login remote host:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!
Erasing Sseries Primary Image, please wait
......!........................................................
...............................................................
..................................................
Verifying erase operation, please wait...Pass.

Programming
...............................................................
...............................................................
..................................................!
61062655 bytes successfully copied
FTOS#
```

4

Control and Monitoring

This chapter contains the commands to configure and monitor the system, including Telnet, file transfer protocol (FTP), and trivial file transfer protocol (TFTP) as they apply to the S5000 switch.

NOTE: The `enable xfp-power-updates` command was deprecated for the S5000. This command was replaced by the `enable optic-info-update interval` command to update information on temperature and power monitoring in the simple network management protocol (SNMP) management information base (MIB).

asf-mode

Enable Alternate Store and Forward (ASF) mode and forward packets as soon as a threshold is reached.

S5000

Syntax

`asf-mode stack-unit {`*`unit-number`*` | all} queue size`

To return to standard Store and Forward mode, use the `no asf-mode stack unit` command.

Parameters

stack-unit *unit-number*	Enter the keywords `stack-unit` followed by the stack-unit number to reset. The range is 0 to 11. Enter `all` to reset all the stack-units. **NOTE:** The S5000 commands accept Unit ID numbers 0 to 11, although the S5000 supports stacking of up to six units with FTOS version 9.0(1.3).
queue size	Enter the queue size of the stack member. The range is 0 to 15.

Defaults

Not configured

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You *must* save the configuration and reload the system to implement ASF. When you enter the command, the system sends a message stating that the new mode is enabled when the system reloads.

banner exec

Configure a message that is displayed when your enter EXEC mode.

S5000

Syntax `banner exec c line c`

Parameters

c	Enter the keywords `banner exec`, then enter a character delimiter, represented here by the letter *c*. Press **ENTER**.
line	Enter a text string for your banner message, ending the message with a delimiter character. In the example below, the delimiter is a percent sign (%). Range: maximum 50 lines, up to 255 characters per line.

Defaults No banner is displayed.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Optionally, use the `banner exec` command to create a text string that is displayed when you access EXEC mode. The `exec-banner` command toggles that display.

Example

```
FTOS(conf)#banner exec ?
LINE c banner-text(max length 255) c, where 'c' is a
delimiting character
FTOS(conf)#banner exec %
Enter TEXT message. End with the character '%'.
This is your banner message.%
FTOS(conf)#end
FTOS#exit
4d21h5m: %STKUNIT0-M:CP %SEC-5-LOGOUT: Exec session is
terminated for user on line
console
This is the banner
FTOS con0 now available
Press RETURN to get started.
4d21h6m: %STKUNIT0-M:CP %SEC-5-LOGIN_SUCCESS: Login successful
for user on line
console
This is the banner
FTOS>
```

Related Commands

banner login – sets a banner for login connections to the system.

banner motd – sets a Message of the Day banner.

exec-banner – Enables the display of a text string when you enter EXEC mode.

line – enables and configures the console and virtual terminal lines to the system.

banner login

Set a banner to be displayed when logging on to the system.

S5000

Syntax

`banner login {keyboard-interactive | no keyboard-interactive} [c line c]`

Parameters

keyboard-interactive	Enter the keyword `keyboard-interactive` to require a carriage return (CR) to get the message banner prompt.
c	Enter the keywords `banner login`, then enter a character delimiter, represented here by the letter *c*. Press **ENTER**.
line	Enter a text string for your banner message, ending the message with a delimiter character. In the example below, the delimiter is a percent sign (%). Range: maximum 50 lines, up to 255 characters per line.

Defaults

No banner is configured and the CR is required when creating a banner.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

A login banner message is displayed only in EXEC Privilege mode after entering the enable command followed by the password. These banners are not displayed to users in EXEC mode.

Example

```
FTOS(conf)#banner login ?
keyboard-interactive Press enter key to get prompt
LINE c banner-text(max length 255) c, where 'c' is a
delimiting character
FTOS(conf)#no banner login ?
keyboard-interactive Prompt will be displayed by default
<cr>
FTOS(conf)#banner login keyboard-interactive
Enter TEXT message. End with the character '%'.
This is your banner message.%
FTOS(conf)#end
FTOS#exit
13d21h9m: %STKUNIT0-M:CP %SEC-5-LOGOUT: Exec session is
terminated for user on line console
This is the banner
FTOS con0 now available
Press RETURN to get started.
13d21h10m: %STKUNIT0-M:CP %SEC-5-LOGIN_SUCCESS: Login
successful for user on line console
This is the banner
```

Related Commands

banner motd – sets a Message of the Day banner.

exec-banner – enables the display of a text string when you enter EXEC mode.

banner motd

Set a message of the day (MOTD) banner.

S5000

Syntax

```
banner motd c line c
```

Parameters

c	Enter the keywords `banner motd`, then enter a character delimiter, represented here by the letter *c*. Press **ENTER**.
line	Enter a text string for your banner message, ending the message with a delimiter character. In the example below, the delimiter is a percent sign (%). Range: maximum 50 lines, up to 255 characters per line.

Defaults

No banner is configured.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

A MOTD banner message is displayed only in EXEC Privilege mode after entering the `enable` command followed by the password. These banners are not displayed to users in EXEC (non-privilege) mode.

Related Commands

banner exec – enables the display of a text string when you enter EXEC mode.

banner login – sets a banner to be displayed after successful login to the system.

cam-audit stack-unit

Enable audit of the IPv4 and IPv6 forwarding table on all stack-units.

Syntax

```
cam-audit stack-unit [all | ipv4-fib | ipv6-fib] interval time-in-minutes
```

Parameters

all	Enter the keyword `all` to enable CAM audit on all stack-units.
ipv4-fib	Enter the keyword `ipv4-fib` to designate the CAM audit on the IPv4 forwarding entries.
ipv6-fib	Enter the keyword `ipv6-fib` to designate the CAM audit on the IPv6 forwarding entries.
interval ***time-in-minutes***	Enter the keyword `interval` followed by the frequency in minutes of the CAM audit. Range: 5 to 1440 minutes (24 hours). Default: **60 minutes**.

Defaults	Disabled
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Enables periodic audits of the software and hardware copies of the IPv4 and IPv6 forwarding tables.

clear alarms

Clear alarms on the system.

S5000

Syntax	`clear alarms`
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	This command clears alarms that are no longer active. If an alarm situation is still active, it is seen in the system output.

clear command history

Clear the command history log.

S5000

Syntax	`clear command history`
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	show command-history – displays a buffered log of all the commands entered by all users along with a time stamp.

clear line

Reset a terminal line.

S5000

Syntax

```
clear line {line-number | console 0 | vty number}
```

Parameters

line-number	Enter a number for one of the 12 terminal lines on the system. Range: 0 to 11.
console 0	Enter the keywords `console 0` to reset the console port.
vty number	Enter the keyword `vty` followed by a number to clear a terminal line. Range: 0 to 9.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

configure

Enter CONFIGURATION mode from EXEC Privilege mode.

S5000

Syntax

```
configure [terminal]
```

Parameters

terminal	(OPTIONAL) Enter the keyword `terminal` to specify that you are configuring from the terminal.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#configure
FTOS(conf)#
```

debug cpu-traffic-stats

Enable the collection of computer processor unit (CPU) traffic statistics.

S5000

Syntax	`debug cpu-traffic-stats`
Defaults	Disabled
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	This command enables (and disables) the collection of CPU traffic statistics from the time this command is executed (not from system boot). However, excessive traffic received by a CPU automatically triggers (turn on) the collection of CPU traffic statics. The following message is an indication that collection of CPU traffic is automatically turned on. To view the traffic statistics, use the `show cpu-traffic-stats` command. If excessive traffic is received by the CPU, traffic will be rate controlled. **NOTE:** This command must be enabled before the `show cpu-traffic-stats` command displays traffic statistics. Dell Networking recommends disabling debugging (`no debug cpu-traffic-stats`) after troubleshooting is complete.
Related Commands	show cpu-traffic-stats – displays the cpu traffic statistics.

debug ftpserver

View transactions during an FTP session when a user is logged into the FTP server.

S5000

Syntax	`debug ftpserver`
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

disable

Return to EXEC mode.

S5000

Syntax `disable [level]`

Parameters

level	(OPTIONAL) Enter a number for a privilege level of the FTOS. Range: 0 to 15. Default: **1**.

Defaults **1**

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

do

Allows the execution of most EXEC-level commands from all CONFIGURATION levels without returning to the EXEC level.

S5000

Syntax `do command`

Parameters

command	Enter an EXEC-level command.

Defaults No default behavior.

Command Modes

- CONFIGURATION
- INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The following commands are *not* supported by the `do` command:

- enable
- disable
- exit
- config

Example

```
FTOS(conf-if-te-5/0)#do clear counters
Clear counters on all interfaces [confirm]
FTOS(conf-if-te-5/0)#
FTOS(conf-if-te-5/0)#do clear logging
Clear logging buffer [confirm]
```

```
FTOS(conf-if-te-5/0)#
FTOS(conf-if-te-5/0)#do reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload [confirm yes/no]: n
FTOS(conf-if-te-5/0)#
```

enable

Enter EXEC Privilege mode or any other privilege level configured. After entering this command, you may need to enter a password.

S5000

Syntax

`enable [level]`

Parameters

level	(OPTIONAL) Enter a number for a privilege level of FTOS. Range: 0 to 15.

Defaults

15

Command Modes

EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Users entering EXEC Privilege mode or any other configured privilege level can access configuration commands. To protect against unauthorized access, use the `enable password` command to configure a password for the `enable` command at a specific privilege level. If no privilege level is specified, the default is privilege level **15**.

Related Commands

enable password – configures a password for the `enable` command and to access a privilege level.

enable optic-info-update interval

Enable polling intervals of optical information updates for simple network management protocol (SNMP).

S5000

Syntax

`enable optical-info-update interval seconds`

To disable optical power information updates, use the `no enable optical-info-update interval` command.

Parameters

interval ***seconds***	Enter the keyword `interval` followed by the polling interval in seconds. Range: 120 to 6000 seconds. Default: **300 seconds** (5 minutes).

Defaults	Disabled
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Use this command to enable polling and to configure the polling frequency.

end

Return to EXEC Privilege mode from other command modes (for example, CONFIGURATION or ROUTER OSPF modes).

S5000

Syntax `end`

Command Modes

- CONFIGURATION
- SPANNING TREE
- MULTIPLE SPANNING TREE
- LINE
- INTERFACE
- TRACE-LIST
- VRRP
- ACCESS-LIST
- PREFIX-LIST
- AS-PATH ACL
- COMMUNITY-LIST
- ROUTER OSPF
- ROUTER RIP
- ROUTER ISIS
- ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands exit – returns to the lower command mode.

exec-banner

Enable the display of a text string when the user enters EXEC mode.

S5000

Syntax	`exec-banner`
Defaults	**Enabled on all lines** (if configured, the banner appears).
Command Modes	LINE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Optionally, use the `banner exec` command to create a text string that is displayed when you access EXEC mode. This command toggles that display.
Related Commands	banner exec – configures a banner to display when entering EXEC mode. line – enables and configures console and virtual terminal lines to the system.

exec-timeout

Set a time interval the system will wait for input on a line before disconnecting the session.

S5000

Syntax

`exec-timeout minutes [seconds]`

Parameters

minutes	Enter the number of minutes of inactivity on the system before disconnecting the current session. Range: 0 to 35791. Default: **10 minutes** for console line; **30 minutes** for VTY line.
seconds	(OPTIONAL) Enter the number of seconds Range: 0 to 2147483. Default: **0 seconds**.

Defaults

10 minutes for console line; **30 minutes** for VTY lines; **0 seconds**

Command Modes

LINE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To remove the time interval, enter `exec-timeout 0 0`.

Example

```
FTOS con0 is now available
Press RETURN to get started.
FTOS>
```

exit

Return to the lower command mode.

S5000

Syntax	`exit`
Command Modes	EXEC Privilege CONFIGURATION LINE, INTERFACE TRACE-LIST PROTOCOL GVRP SPANNING TREE MULTIPLE SPANNING TREE MAC ACCESS LIST ACCESS-LIST AS-PATH ACL COMMUNITY-LIST PREFIX-LIST ROUTER OSPF ROUTER RIP ROUTER ISIS ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	end – returns to EXEC Privilege mode.

ftp-server enable

Enable FTP server functions on the system.

S5000

Syntax	`ftp-server enable`
Defaults	Disabled
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
morpheus% ftp 10.31.1.111
Connected to 10.31.1.111.
220 FTOS (1.0) FTP server ready
Name (10.31.1.111:dch): dch
331 Password required
Password:
230 User logged in
ftp> pwd
257 Current directory is "flash:"
ftp> dir
200 Port set okay
150 Opening ASCII mode data connection
size  date         time     name
--------------------------------------
512   Jul-20-2004  18:15:00 tgtimg
512   Jul-20-2004  18:15:00 diagnostic
512   Jul-20-2004  18:15:00 other
512   Jul-20-2004  18:15:00 tgt
226 Transfer complete
329 bytes received in 0.018 seconds (17.95 Kbytes/s)
ftp>
```

Related Commands

ftp-server topdir – sets the directory to be used for incoming FTP connections to the S5000.

ftp-server username – sets a username and password for incoming FTP connections to the S5000.

ftp-server topdir

Specify the top-level directory to be accessed when an incoming FTP connection request is made.

S5000

Syntax

`ftp-server topdir *directory*`

Parameters

directory	Enter the directory path.

Defaults

The internal flash is the default directory.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

After you enable FTP server functions with the `ftp-server enable` command, Dell Networking recommends that you specify a top-level directory path. Without a top-level directory path specified, the FTOS directs users to the flash directory when logging in to the FTP server.

Related Commands

ftp-server topdir – sets the directory to be used for incoming FTP connections to the S5000.

ftp-server username – sets a username and password for incoming FTP connections to the S5000.

ftp-server username

Create a user name and associated password for incoming FTP server sessions.

S5000

Syntax

`ftp-server username username password [encryption-type] password`

Parameters

username	Enter a text string up to 40 characters long as the user name.
password *password*	Enter the keyword `password` followed by a string up to 40 characters long as the password. Without specifying an encryption type, the password is unencrypted.
encryption-type	(OPTIONAL) After the keyword `password`, enter one of the following numbers: • `0` (zero) for an unecrypted (clear text) password • `7` (seven) for a hidden text password

Defaults Not enabled.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

ftp-server topdir – sets the directory to be used for incoming FTP connections to the S5000.

ftp-server username – sets a username and password for incoming FTP connections to the S5000.

hostname

Set the host name of the system.

S5000

Syntax

`hostname name`

Parameters

name	Enter a text string, up to 32 characters long.

Defaults FTOS

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	The hostname is used in the prompt.

ip ftp password

Specify a password for outgoing FTP connections.

S5000

Syntax	`ip ftp password [`*`encryption-type`*`]` *`password`*
Parameters	

encryption-type	(OPTIONAL) Enter one of the following numbers: • `0` (zero) for an unecrypted (clear text) password • `7` (seven) for a hidden text password
password	Enter a string up to 40 characters as the password.

Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	The password is listed in the configuration file; you can view the password by entering the `show running-config ftp` command. The password configured by the `ip ftp password` command is used when you use the `ftp: parameter` in the `copy` command.
Related Commands	copy – copy files. ip ftp username – sets the user name for the FTP sessions.

ip ftp source-interface

Specify an interface's IP address as the source IP address for FTP connections.

S5000

Syntax	`ip ftp source-interface` *`type slot/port`*
Parameters	

source-interface*type slot/port*	Enter the `source-interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below.

- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults The IP address on the system that is closest to the Telnet address is used in the outgoing packets.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands copy – copies files from and to the switch.

ip ftp username

Assign a user name for outgoing FTP connection requests.

S5000

Syntax `ip ftp username username`

Parameters

username	Enter a text string as the user name up to 40 characters long.

Defaults No user name is configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information You must also configure a password with the `ip ftp password` command.

Related Commands ip ftp password – sets the password for FTP connections.

ip telnet server enable

Enable the Telnet server on the switch.

S5000

Syntax `ip telnet server enable`

Defaults Enabled

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands ip ssh server – enables the secure shell (SSH) server on the system.

ip telnet source-interface

Set an interface's IP address as the source address in outgoing packets for Telnet sessions.

S5000

Syntax `ip telnet source-interface` *`type slot/port`*

Parameters

source-interface*type slot/port*	Enter the `source-interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults The IP address on the system that is closest to the Telnet address is used in the outgoing packets.

Command Modes CONFIGURATION

Command History	
Version 9.0(1.3)	Introduced on the S5000.

Related Commands telnet – telnets to another device.

ip tftp source-interface

Assign an interface’s IP address in outgoing packets for TFTP traffic.

S5000

Syntax `ip tftp source-interface` *`type slot/port`*

Parameters

source-interface*type slot/port*	Enter the `source-interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults The IP address on the system that is closest to the Telnet address is used in the outgoing packets.

Command Modes CONFIGURATION

Command History	
Version 9.0(1.3)	Introduced on the S5000.

line

Enable and configure console and virtual terminal lines to the system. This command accesses LINE mode, where you can set the access conditions for the designated line.

S5000

Syntax	`line {console 0	vty number [end-number]}`
Parameters	

console 0	Enter the keyword `console 0` to configure the console port. The console option for the S5000 is `<0-0>`.
vty *number*	Enter the keyword `vty` followed by a number from 0 to 9 to configure a virtual terminal line for Telnet sessions. The system supports 10 Telnet sessions.
end-number	(OPTIONAL) Enter a number from 1 to 9 as the last virtual terminal line to configure. You can configure multiple lines at one time.

Defaults	Not configured
Command Modes	CONFIGURATION
Command History	

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	You cannot delete a terminal connection.
Related Commands	access-class – restricts the incoming connections to a particular IP address in an IP access control list (ACL). password – specifies a password for users on terminal lines.

motd-banner

Enable a message of the day (MOTD) banner to appear when you log in to the system.

S5000

Syntax	`motd-banner`
Defaults	Enabled on all lines.
Command Modes	LINE
Command History	

Version 9.0(1.3)	Introduced on the S5000.

ping

Test connectivity between the system and another device by sending echo requests and waiting for replies.

S5000

Syntax

```
ping [host | ip-address | [count {number | continuous}]
[datagram-size] [timeout] [ip src-ipv4-address | source-
interface-type slot/port] [tos] [df-bit (y|n)] [validate-
reply(y|n)] [outgoing-interface] [pattern pattern] [sweep-min-
size] [sweep-max-size] [sweep-interval] [outgoing-interface (ip
src-ipv4-address) | outgoing-interface-type slot/port]
```

Parameters

host	(OPTIONAL) Enter the host name of the devices to which you are testing connectivity.
ip-address	(OPTIONAL) Enter the IPv4 address of the device to which you are testing connectivity. The address must be in the dotted decimal format.
count	Enter the number of echo packets to be sent. Default: **5**. • number: 1- 2147483647 • continuous: transmit echo request continuously
datagram size	Enter the ICMP datagram size. Range: 36 - 15360 bytes. Default: **100**.
timeout	Enter the interval to wait for an echo reply before timing out. Range: 0 -3600 seconds. Default: **2 seconds**.
source-interface-type slot/port	Enter the IPv4 source ip address or the source interface. Enter the IP address in A.B.C.D format. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
tos	(IPv4 only) Enter the type of service required. Range: 0-255. Default: **0**.
df-bit	(IPv4 only) Enter `Y` or `N` for the “don't fragment” bit in IPv4 header. • `N`: Do not set the “don't fragment” bit. • `Y`: Do set “don't fragment” bit Default is **No**.
validate-reply	(IPv4 only) Enter `Y` or `N` for reply validation.

	- `N`: Do not validate reply data . - `Y`: Do validate reply data . Default is `No`.
outgoing-interface	Enter the outgoing interface for ping packets to a destination link-local address.
pattern *pattern*	(IPv4 only) Enter the IPv4 data pattern. Range: 0-FFFF. Default: 0xABCD.
sweep-min-size	Enter the minimum size of datagram in sweep range. Range: 52-15359 bytes.
sweep-max-size	Enter the maximum size of datagram in sweep range. Range: 53-15359 bytes.
sweep-interval	Enter the incremental value for sweep size. Range: 1-15308 seconds.
outgoing-interface-type slot/port	(IPv4 only) Enter the outgoing interface for multicast packets. Enter the IP address in A.B.C.D format. - For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. - For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. - For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you enter the `ping` command without specifying an IP/IPv6 address (Extended Ping), you are prompted for a target IP/IPv6 address, a repeat count, a datagram size (up to 1500 bytes), a timeout (in seconds), and for Extended Commands. For information on the ICMP message codes that return from a `ping` command, refer to ICMP Message Types.

The following table provides descriptions for the `ping` command status response symbols displayed in the output.

Symbol	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates the network server timed out while waiting for a reply.

U	A destination unreachable error PDU was received.
Q	Source quench (destination too busy).
M	Could not fragment.
?	Unknown packet type.
&	Packet lifetime exceeded.

Example (IPv4)

```
FTOS#ping 172.31.1.255

Type Ctrl-C to abort.

Sending 5, 100-byte ICMP Echos to 172.31.1.255, timeout is 2
seconds:
Reply to request 1 from 172.31.1.208 0 ms
Reply to request 1 from 172.31.1.216 0 ms
Reply to request 1 from 172.31.1.205 16 ms
::
Reply to request 5 from 172.31.1.209 0 ms
Reply to request 5 from 172.31.1.66 0 ms
Reply to request 5 from 172.31.1.87 0 ms
FTOS#
```

Example (IPv6)

```
FTOS#ping 100::1

Type Ctrl-C to abort.

Sending 5, 100-byte ICMP Echos to 100::1, timeout is 2 seconds:
!!!!!
Success rate is 100.0 percent (5/5), round-trip min/avg/max =
0/0/0 (ms)
FTOS#
```

reload

Reboot FTOS.

S5000

Syntax `reload`

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If there is a change in the configuration, FTOS prompts you to save the new configuration. Or you can save your running configuration with the `copy running-config` command.

Related Commands reset stack-unit – resets any designated stack member except the management unit.

send

Send messages to one or all terminal line users.

S5000

Syntax

```
send [*] | [line ] | [console] | [vty]
```

Parameters

*****	Enter the asterisk character `*` to send a message to all tty lines.
line	Send a message to a specific line. Range: 0 to 11.
console	Enter the keyword `console` to send a message to the primary terminal line.
vty	Enter the keyword `vty` to send a message to the virtual terminal.

Defaults none

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Messages can contain an unlimited number of lines; however, each line is limited to 255 characters. To move to the next line, use the `<CR>`. To send the message use `CTR-Z`;to abort a message use `CTR-C`.

service timestamps

Add time stamps to debug and log messages. This command adds either the uptime or the current time and date.

S5000

Syntax

```
service timestamps [debug | log] [datetime [localtime] [msec]
[show-timezone] | uptime]
```

Parameters

debug	(OPTIONAL) Enter the keyword `debug` to add timestamps to debug messages.
log	(OPTIONAL) Enter the keyword `log` to add timestamps to log messages with severity 0 to 6.
datetime	(OPTIONAL) Enter the keyword `datetime` to have the current time and date added to the message.
localtime	(OPTIONAL) Enter the keyword `localtime` to include the localtime in the timestamp.
msec	(OPTIONAL) Enter the keyword `msec` to include milliseconds in the timestamp.

show-timezone	(OPTIONAL) Enter the keyword `show-timezone` to include the time zone information in the timestamp.
uptime	(OPTIONAL) Enter the keyword `uptime` to have the timestamp based on time elapsed since system reboot.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you do not specify parameters and enter service timestamps, it appears as service timestamps debug uptime in the running-configuration.

Use the `show running-config` command to view the current options set for the `service timestamps` command.

show alarms

View alarms for the stack-unit, switch, and fan trays.

S5000

Syntax `show alarms [threshold]`

Parameters

threshold	(OPTIONAL) Enter the keyword `threshold` to display the temperature thresholds set for the stack-unit.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show alarms

--  Minor Alarms  --
Alarm Type                                 Duration
-------------------------------------------------------------
No minor alarms

--  Major Alarms  --
Alarm Type                                 Duration
-------------------------------------------------------------
fan tray 0 in unit 0 failed or removed  3 day, 23 hr, 6 min
fan tray 3 in unit 0 failed or removed  3 day, 23 hr, 6 min
FTOS#
```

show command-history

Display a buffered log of all commands entered by all users along with a time stamp.

S5000

Syntax `show command-history`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show command-history
[4/30 10:6:38]: CMD-(TEL0):[enable]by admin from vty0
(10.11.51.14)
[4/30 10:6:51]: CMD-(TEL0):[show version]by admin from vty0
(10.11.51.14)
[4/30 10:8:6]: CMD-(TEL0):[configure]by admin from vty0
(10.11.51.14)
         - Repeated 1 time.
[4/30 10:10:7]: CMD-(TEL0):[no banner login keyboard-
interactive]by admin from vty0 (10.11.51.14)
[4/30 10:11:7]: CMD-(TEL0):[interface tengigabitethernet
1/1]by admin from vty0 (10.11.51.14)
[4/30 10:11:18]: CMD-(TEL0):[clear counters]by admin from vty0
(10.11.51.14)
[4/30 10:12:51]: CMD-(TEL0):[exit]by admin from vty0
(10.11.51.14)
[4/30 10:13:52]: CMD-(TEL0):[ping 100::1]by admin from vty0
(10.11.51.14)
[4/30 10:14:34]: CMD-(TEL0):[show alarms]by admin from vty0
(10.11.51.14)
[4/30 10:14:55]: CMD-(TEL0):[show command-history]by admin
from vty0 (10.11.51.14)
         - Repeated 1 time.
FTOS#
```

Related Commands clear command history – clears the command history log.

show command-tree

Display the entire CLI command tree, and optionally, display the utilization count for each commands and its options.

S5000

Syntax `show command-tree [count | no]`

Parameters

count	Display the command tree with a usage counter for each command.
no	Display all of the commands that may be preceded by the keyword `no`, which is the keyword used to remove a command from the running-configuration.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Reload the system to reset the command-tree counters.

Example

```
FTOS#show command-tree count
!
Enable privilege mode:

clear counters                          command usage:3
  fibrechannel                                  option
usage:     0
  SLOT/PORT                                     option
usage:     0
fortyGigE                                       option
usage:     0
  SLOT/PORT                                     option
usage:     0
   learning-limit                               option
usage:     0
   vrrp                                         option
usage:     0
    <1-255>                                     option
usage:     0
    ipv6                                        option
usage:     0
     <1-255>                                    option
usage:     0
gigabitethernet                                 option
usage:     0
  SLOT/PORT                                     option
usage:     0
   learning-limit                               option
usage:     0
   vrrp                                         option
usage:     0
    <1-255>                                     option
usage:     0
    ipv6                                        option
usage:     0
     <1-255>                                    option
usage:     0
ip                                              option
usage:     0
  access-group                                  option
usage:     0
   WORD                                         option
```

```
usage:     0
   WORD                                         option
usage:     0
ipv6                                            option
usage:     0
  access-group                                  option
usage:     0
   WORD                                         option
usage:     0
learning-limit                                  option
usage:     0
loopback                                        option
usage:     0
  <0-16383>                                     option
usage:     0
mac                                             option
usage:     0
  access-group                                  option
usage:     0
   WORD                                         option
usage:     0
    in                                          option
usage:     0
    out                                         option
usage:     0
managementethernet                              option
usage:     0
  SLOT/PORT                                     option
usage:     0
port-channel                                    option
usage:     0
  <1-128>                                       option
usage:     0
   learning-limit                               option
usage:     0
   vrrp                                         option
usage:     0
    <1-255>                                     option
usage:     0
    ipv6                                        option
usage:     0
     <1-255>                                    option
usage:     0
   learning-limit                               option
usage:     0
tengigabitethernet                              option
usage:     0
  SLOT/PORT                                     option
usage:     0
   learning-limit                               option
usage:     0
   vrrp                                         option
usage:     0
    <1-255>                                     option
usage:     0
    ipv6                                        option
usage:     0
     <1-255>                                    option
usage:     0
  <1-16383>                                     option
usage:     0
  <1-4094>                                      option
usage:     0
   vrrp                                         option
```

```
usage:     0
    <1-255>                                     option
usage:     0
    ipv6                                        option
usage:     0
     <1-255>                                    option
usage:     0
vrrp                                            option
usage:     0
  <1-255>                                       option
usage:     0
  ipv6                                          option
usage:     0
   <1-255>                                      option
usage:     0

enable                                   command usage:1
  <0-15>                                         option
usage:     0

ping                                     command usage:2
  ethernet                                      option
usage:     0
  domain                                        option
usage:     0
   level                                        option
usage:     0
    <0-7>                                       option
usage:     0
     ma-name                                    option
usage:     0
      name                                      option
usage:     0
<------------- output truncated ----------->
```

show cpu-traffic-stats

View the CPU traffic statistics.

S5000

Syntax `show cpu-traffic-stats [port number | all ]`

Parameters

port number	(OPTIONAL) Enter the port number to display traffic statistics on that port only. Range: 1 to 1568.
all	(OPTIONAL) Enter the keyword `all` to display traffic statistics on all the interfaces receiving traffic, sorted based on the traffic.

Defaults all

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	Traffic statistics are sorted on a per-interface basis; the interface receiving the most traffic is displayed first. All CPU and port information is displayed unless a specific port or CPU is specified. Traffic information is displayed for router ports only; not for management interfaces. The traffic statistics are collected only after the `debug cpu-traffic-stats` command is executed; not from the system bootup. **NOTE:** After debugging is complete, use the `no debug cpu-traffic-stats` command to shut off traffic statistics collection.

Example

```
FTOS#show cpu-traffic-stats
Processor : CP
--------------
   Received 100% traffic on TenGigabitEthernet 7/12   Total 
packets:304392
       LLC:0, SNAP:0, IP:0, ARP:0, other:304392
       Unicast:0, Multicast:304392, Broadcast:0
FTOS#
```

Related Commands	debug cpu-traffic-stats – enables CPU traffic statistics for debugging.

show debugging

View a list of all enabled debugging processes.

S5000

Syntax	`show debugging`
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
FTOS#show debug
Generic IP:
  IP packet debugging is on for
    ManagementEthernet 0/0
    Port-channel 1-2
    Port-channel 5
    TenGigabitEthernet 4/0-3,5-6,10-11,20
    TenGigabitEthernet 5/0-1,5-6,10-11,15,17,19,21
  ICMP packet debugging is on for
    TenGigabitEthernet 5/0,2,4,6,8,10,12,14,16
FTOS#
```

show environment

View S5000 system component status (for example, temperature or voltage).

S5000

Syntax `show environment [all | fan | stack-unit` *`unit-number`* `| pem]`

Parameters

all	Enter the keyword `all` to view all components.
fan	Enter the keyword `fan` to view only information on fans. The output of this command is chassis dependent.
stack-unit ***unit-number***	Enter the keyword `stack-unit` followed by a number to view only information on a stack-unit. The range is 0 to 11.
pem	Enter the keyword `pem` to view only information on power entry modules.

Command Modes

- EXEC
- EXEC Privildge

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The example below shows the output of the `show environment all` command. You can also display status for individual components.

Example (all)

```
FTOS#show environment all

--  Fan  Status  --
Unit Bay   TrayStatus  Fan0    Speed   Fan1    Speed   Fan2
Speed   Fan3    Speed
---------------------------------------------------------------
-----------------------
1    1     up          up      12000   up      12000   up
12000   up      12000
1    2     up          up      12000   up      12000   up
12000   up      12000

Speed in RPM

--  Power Supplies  --
Unit   Bay   Status       Type    FanStatus
---------------------------------------------------------------
-------------
  1     0    up           AC      up
  1     3    up           AC      up

--  Thermal Sensor Readings (degree C)  --

-- Unit 1 --
             S0    S1    S2    S3    S4    S5    S6    S7
---------------------------------------------------------------
---------------------------------------
BASE BOARD   40    33    29    33    31    49    33    43
Module 0     31    35    34    -     -     -     -     -
Module 1     -     -     -     -     -     -     -     -
Module 2     -     -     -     -     -     -     -     -
Module 3     -     -     -     -     -     -     -     -
```

show inventory

Display the S5000 switch type, components (including media), and FTOS version including hardware identification numbers and configured protocols.

S5000

Syntax `show inventory [media slot]`

Parameters

media *slot*	(OPTIONAL) Enter the keyword `media` followed by the stack ID of the stack member you want to display pluggable media inventory.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If there are no fiber ports in the unit, just the header under `show inventory media` is displayed. If there are fiber ports but no optics inserted, the output displays "Media not present or accessible".

Example

```
FTOS#  show inventory
System Type            : S5000
System Mode            : 3.0
Software Version       : 9.0(1.3)

Unit Type                       Serial Number  Part Number
Rev  Piece Part ID            Rev  Svc Tag  Exprs Svc Code
---------------------------------------------------------------
----------------------------------------------------
* 0  S5000                      TYUS01BA0269   0K9N70
00A  US-0K9N70-76991-1BA-0269 00A  DQX74S1  299 260 510 57
  0  S5000-MOD-12xFC8ETH10-U    ZPTW031F0001   75200101
00A  TW-0Y0W01-75412-31F-0001 00A  CCQ22S1  268 907 490 73
  0  S5000-MOD-12xETH10-F       ZPTW031F0002   75200102
00A  TW-0Y0W02-75412-31F-0002 00A  CCQ22S2  268 907 490 74
  0  S5000-MOD-12xETH10-F       TYUS01BA0260   0K9N60
00A  US-0K9N60-76991-1BA-0260 00A  FCT00G1  334 260 385 93
  0  S5000-MOD-12xETH10-F       TYUS01BA0261   0K9N61
00A  US-0K9N61-76991-1BA-0261 00A  FCT00G2  334 260 385 94
  0  S5000-PWR-AC               NA             0V4JC6X01
X01  CN-0V4JC6-73245-29J-0078 N/A  N/A      0
  0  S5000-PWR-AC               NA             0XTVK2X01
X01  CN-0XTVK2-17972-29R-004K N/A  N/A      0
  0  S5000-FAN                  ZPTW031F0009   7500000129
00A  TW-0L0M09-75412-31F-0009 00A  BCQ22S9  247 139 667 45
  0  S5000-FAN                  TYUS01BA0007   0K0007
00A  US-0K0007-76991-1BA-0007 00A  DCT00B7  290 724 737 47
```

```
* - Management Unit

Software Protocol Configured
--------------------------------------------------------------
  DCBX
  LLDP
  SNMP

FTOS#
```

Example (media)

```
FTOS#show inventory media
Slot   Port     Type        Media              Serial
Number        F10Qualified
---------------------------------------------------------------
---------------
   1      0          Media not present or accessible
   1      1          Media not present or accessible
   1      2          Media not present or accessible
   1      3          Media not present or accessible
   1      4     UNKNOWN     UNKNOWN
PNJ2R98                  Yes
   1      5     SFP+        10GBASE-CU7M
APF10520050667           Yes
   1      6     UNKNOWN     UNKNOWN
CCX111430001545          No
   1      7     UNKNOWN     UNKNOWN
UJM03PM                  Yes
   1      8          Media not present or accessible
   1      9     SFP+        10GBASE-CU1M
APF11380028W68           Yes
   1     10     SFP         1000BASE-SX
PMM6PG1                  Yes
   1     11     SFP         1000BASE-SX
PMM6N25                  Yes
   1     48     QSFP        40GBASE-CR4-1M
APF12310017UL7           Yes
   1     52     QSFP        40GBASE-CR4-5M
APF114800218NL           Yes
   1     56     QSFP        40GBASE-CR4-1M
APF11490011J2P           Yes
   1     60          Media not present or accessible

FTOS#
```

Related Commands

show interfaces – displays a specific interface configuration.

show interfaces transceiver – displays the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

show processes cpu

Display CPU usage information based on processes running in an S5000.

S5000

Syntax

```
show processes cpu [management-unit 1-99 [details] | stack-unit
unit-number | summary | ipc | memory [stack-unit 0-11]]
```

Parameters

management-unit *1-99*	(OPTIONAL) Display processes running in the control processor. The `1-99` variable sets the number of tasks to display in order of the highest CPU usage in the past five (5) seconds.
details	Display all running processes (except sysdlp). Refer to Example (management-unit).
stack-unit *unit-number*	(OPTIONAL) Enter the keyword `stack-unit` followed by a number. The range is 0 to 11.
summary	(OPTIONAL) Enter the keyword `summary` to view a summary view of CPU usage for all members of the stack. Refer to Example (summary).
ipc	(OPTIONAL) Enter the keyword `ipc` to display inter-process communication statistics.
memory	(OPTIONAL) Enter the keyword `memory` to display memory statistics. Refer to Example (memory).

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (summary)

```
FTOS#show processes cpu summary

 CPU utilization  5Sec 1Min 5Min
 -----------------------------------------
 UNIT0              6%   6%   5%
FTOS#
```

Example (management-unit)

```
FTOS#show processes cpu management-unit

CPU utilization for five seconds: 15%/0%; one minute: 14%;
five minutes: 14%
PID        Runtime(ms)    Invoked        uSecs     5Sec
1Min     5Min   TTY          Process
0x00000000       10610        1061       10000    8.00%
8.00%    8.00%   0            system
0x00000136    31767650     3176765       10000    6.90%
6.52%    6.48%   0            sysdlp
0x0000012f     1123270      112327       10000    0.39%
0.20%    0.26%   0              sysd
0x000000f1      124940       12494       10000    0.20%
0.07%    0.03%   0              igmp
0x000001bd       40560        4056       10000    0.20%
```

```
0.02%    0.00%   0              frrp
0x0000015f       46350        4635       10000    0.00%
0.02%    0.01%   0              vrrp
0x0000015d       22610        2261       10000    0.00%
0.02%    0.01%   0               rip
0x00000075      104770       10477       10000    0.00%
0.02%    0.01%   0               pim
0x00000015       64740        6474       10000    0.00%
0.02%    0.02%   0         mount_mfs
0x000001a9       27080        2708       10000    0.00%
0.00%    0.01%   0             l2mgr
0x0000013f       24410        2441       10000    0.00%
0.00%    0.01%   0               acl
0x00000148       25600        2560       10000    0.00%
0.00%    0.01%   0           mlagmgr
0x000001ad       26720        2672       10000    0.00%
0.00%    0.01%   0              mrtm
0x0000014c       26230        2623       10000    0.00%
0.00%    0.01%   0              ipm1
0x00000190       26010        2601       10000    0.00%
0.00%    0.00%   0              ndpm
0x0000019c       22530        2253       10000    0.00%
0.00%    0.00%   0               otm
0x00000144       24350        2435       10000    0.00%
0.00%    0.00%   0              l2pm
0x00000173       26850        2685       10000    0.00%
0.00%    0.00%   0               dsm
0x00000159       25230        2523       10000    0.00%
0.00%    0.00%   0              xstp
0x00000132         180          18       10000    0.00%
0.00%    0.00%   0            sysmon
0x00000124        3300         330       10000    0.00%
0.00%    0.00%   0         flashmntr
0x000000e8          10           1       10000    0.00%
0.00%    0.00%   0         mount_mfs
0x000000e5          40           4       10000    0.00%
0.00%    0.00%   0         mount_mfs
0x000000d8          10           1       10000    0.00%
0.00%    0.00%   0             inetd
0x00000091          90           9       10000    0.00%
0.00%    0.00%   0                sh
0x0000004e          80           8       10000    0.00%
0.00%    0.00%   0                sh
0x00000023         120          12       10000    0.00%
0.00%    0.00%   0         mount_mfs
0x000000db       25540        2554       10000    0.00%
0.00%    0.00%   0              arpm
0x00000002          80           8       10000    0.00%
0.00%    0.00%   0                sh
0x00000001          10           1       10000    0.00%
0.00%    0.00%   0              init
0x00000157       58820        5882       10000    0.00%
0.00%    0.00%   0              lacp
0x0000016b       24480        2448       10000    0.00%
0.00%    0.01%   0               rtm
FTOS#
```

Example (stack-unit)

```
FTOS#show processes cpu stack-unit 0

CPU utilization for five seconds:5%/0%;one minute:6%;five
minutes:4%
PID        Run      Invoked uSecs 5Sec  1Min  5Min  TTY
Process
```

```
           time(ms)
0x42ada000 18821340 1882134 10000 5.00% 6.00% 4.97%  0
KP
0x42bd2000        0       0     0 0.00% 0.00% 0.00%  0
debugagt
0x42bb0000       20       2 10000 0.00% 0.00% 0.00%  0
F10StkMgr
0x42b8d000   106090   10609 10000 0.00% 0.00% 0.00%  0
lcMgr
0x42b68000     2470     247 10000 0.00% 0.00% 0.00%  0
dla
0x42b43000    48300    4830 10000 0.00% 0.00% 0.00%  0
sysAdmTsk
0x42b21000   263260   26326 10000 0.00% 0.00% 0.00%  0
timerMgr
0x42b00000   109090   10909 10000 0.00% 0.00% 0.00%  0
PM
0x42bf4000    19020    1902 10000 0.00% 0.00% 0.00%  0
diagagt
0x42ab6000       10       1 10000 0.00% 0.00% 0.00%  0
evagt
0x42a8f000    10880    1088 10000 0.00% 0.00% 0.00%  0
ipc
0x41d95000      180      18 10000 0.00% 0.00% 0.00%  0
tme
0x41d6a000       80       8 10000 0.00% 0.00% 0.00%  0
tDDB
0x41d68000      840      84 10000 0.00% 0.00% 0.00%  0
GC
0x41d49000        0       0     0 0.00% 0.00% 0.00%  0
isrTask
0x41d2b000       10       1 10000 0.00% 0.00% 0.00%  0
tSysLog
0x41d27000   350400   35040 10000 0.00% 0.00% 0.00%  0
tExcTask
!-------------------output truncated ---------------------!
```

Related Commands

show hardware layer2 acl – displays Layer 2 ACL data for the selected stack member and stack member port-pipe.

show hardware layer3 – displays Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

show hardware stack-unit – displays the data plane or management plane input and output statistics of the designated component of the designated stack member.

show hardware system-flow – displays Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

show interfaces stack-unit – displays information on all interfaces on a specific S5000 stack member.

show processes memory – displays CPU usage information based on processes running in an S5000 switch.

show processes ipc flow-control

Display the single window protocol queue (SWPQ) statistics.

S5000

Syntax

```
show processes ipc flow-control [cp]
```

Parameters

cp	(OPTIONAL) Enter the keyword `cp` to view the control processor's SWPQ statistics.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Field	**Description**
Tx Process	Source Service Identifier
Rx Process	Destination Service Identifier
Cur Len	Current number of messages enqueued
High Mark	Highest number of packets in the queue at any point of time
Timeout	Timeout count
Retries	Number of retransmissions
Msg Sent	Number of messages sent
Ack Rcvd	Number of messages acknowledged
Aval Retra	Number of retries left/available
Max Retra	Number of retries allowed

Important Points:

- The SWP provides flow control-based reliable communication between the sending and receiving software tasks.
- A sending task enqueues messages into the SWP queue3 for a receiving task and waits for an acknowledgement.
- If no response is received within a defined period of time, the SWP timeout mechanism resubmits the message at the head of the FIFO queue.
- After retrying a defined number of times, the `SWP-2-NOMORETIMEOUT` timeout message is generated.
- In the example, a retry (Retries) value of zero indicates that the SWP mechanism reached the maximum number of retransmissions without an acknowledgement.

Example

```
FTOS#show processes ipc flow-control

Q Statistics on CP Processor
    TxProcess     RxProcess       Cur        High   Time
Retr       Msg       Ack  Aval   Max
                                  Len        Mark   Out
ies       Sent      Rcvd Retra Retra
         ACL0          RTM0         0          0      0
0         0         0    10    10
         ACL0     DIFFSERV0         0          0      0
0         0         0    10    10
         ACL0         IGMP0         0          0      0
0         0         0    10    10
         ACL0          PIM0         0          0      0
0         0         0    10    10
      ARPMGR0         MRTM0         0          0      0
0         0         0   100   100
        LACP0        IFMGR0         0          0      0
0         0         0    25    25
         RTM0          OTM0         0          0      0
0         0         0    60    60
         RTM0          OTM0         0          0      0
0         0         0    60    60
         RTM0       ARPMGR0         0          0      0
0         0         0   136   136
       IFMGR0         FEFD0         0          1      0
0         4         4    60    60
       IFMGR0 EVENTTERMLOG0         0          1      0
0         1         1    60    60
       IFMGR0        IPMGR0         0          3      0
0         5         5    60    60
       IFMGR0         SNMP0         0          1      0
0         1         1    60    60
       IFMGR0       SFL_CP0         0          2      0
0         5         5    60    60
       IFMGR0     PORTMIRR0         0          1      0
0         2         2    60    60
       IFMGR0       IFAGT12         0          1      0
0         1         1    60    60
         OTM0       ARPMGR0         0          0      0
0         0         0    25    25
         OTM0         NDPM0         0          0      0
0         0         0    25    25
         OTM0          RTM0         0          0      0
0         0         0   100   100
         OTM0          RTM0         0          0      0
0         0         0   100   100
      ARPMGR0          OTM0         0          0      0
0         0         0   100   100
       IFMGR0         MRTM0         0          1      0
0         4         4    60    60
         ACL0        IPMGR0         0          0      0
0         0         0    10    10
        FRRP0         L2PM0         0          0      0
0         0         0    25    25
         STP0         L2PM0         0          0      0
0         0         0    25    25
         RTM0        IPMGR0         0          0      0
0         0         0   255   255
       IFMGR0         LACP0         0          2      0
0         5         5    60    60
         ACL0         SNMP0         0          0      0
0         0         0    10    10
```

```
         ACL0        IPMGR0          0          0      0
0         0         0    10    10
         RTM0        IPMGR0          0          0      0
0         0         0   255   255
       IFMGR0          RTM0          0          1      0
0         4         4    60    60
      ARPMGR0        IPMGR0          0          0      0
0         0         0   100   100
       !-------------------output truncated
---------------------!
FTOS#
```

show memory

View current memory usage on the S5000 switch.

S5000

Syntax

`show memory [stack-unit unit-number]`

Parameters

stack-unit *unit-number*	(OPTIONAL) Enter the keyword `stack-unit` followed by a number. The range is 0 to 11.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The output for `show memory` displays the memory usage of LP part (sysdlp) of the system. The sysdlp is an aggregate task that handles all the tasks running on the S5000 CPU.

Example

```
FTOS#show memory stack-unit 0
Statistics On Unit 0 Processor
===========================
Total(b)  Used(b) Free(b)   Lowest(b) Largest(b)
268435456 4010354 264425102 264375410 264425102
```

show processes memory

Display memory usage information based on processes running in the S5000 switch.

S5000

Syntax

`show processes memory {management-unit | stack unit {0-11 | all | summary}}`

Parameters

management-unit	Enter the keyword `management-unit` for CPU memory usage of the stack management unit.
stack unit *0–11*	Enter the keyword `stack unit` followed by a stack unit number for which to display memory usage on the forwarding processor.
all	Enter the keyword `all` for detailed memory usage on all stack members.
summary	Enter the keyword `summary` for a brief summary of memory availability and usage on all stack members.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `show processes memory` output fields are described below:

Field	**Description**
Total:	Total system memory available
MaxUsed:	Total maximum memory used ever (history indicated with time stamp)
CurrentUsed:	Total memory currently in use
CurrentFree:	Total system memory available
SharedUsed:	Total used shared memory
SharedFree:	Total free shared memory
PID	Process ID
Process	Process Name
ResSize	Actual resident size of the process in memory
Size	Process test, stack, and data size
Allocs	Total dynamic memory allocated
Frees	Total dynamic memory freed
Max	Maximum dynamic memory allocated
Current	Current dynamic memory in use

The output for the `show process memory` command displays the memory usage statistics running on CP part (sysd) of the system. The sysd is an aggregate task that handles all the tasks running on S5000 CP.

The output of the `show memory` command and this command differ based on which FTOS processes are counted.

- In the `show memory` output, the memory size is equal to the size of the application processes.

- In the output of this command, the memory size is equal to the size of the application processes plus the size of the system processes.

Example (memory)

```
FTOS#show processes memory

     Memory Statistics Of Stack Unit 1 (bytes)

===========================================================
Total:  2147483648, MaxUsed:   401354752, CurrentUsed:
401354752, CurrentFree:  1746128896
    TaskName      TotalAllocated       TotalFreed
MaxHeld    CurrentHolding
    f10appioserv          188416              0
0          106496
            ndpm          630784              0
0         5255168
    f10appioserv          188416              0
0          139264
         mlagmgr          114688              0
0         4861952
    f10appioserv          188416              0
0          122880
            vrrp          323584              0
0         5451776
    f10appioserv          188416              0
0          139264
            frrp          184320              0
0         5042176
    f10appioserv          188416              0
0          118784
            xstp         4513792              0
0         9207808
    f10appioserv          188416              0
0          139264
             pim          950272              0
0         5345280
    f10appioserv          188416              0
0          139264
            igmp          499712              0
0         5365760
    f10appioserv          188416              0
0          118784
            mrtm         5943296              0
0        11030528
    f10appioserv          188416              0
0          106496
           l2mgr          950272              0
0        20856832
    f10appioserv          188416              0
0          139264
            l2pm          188416              0
0         5165056
    f10appioserv          188416              0
0          139264
            arpm          446464              0
0         4796416
    f10appioserv          188416              0
0          139264
             otm          184320              0
0         4927488
    f10appioserv          188416              0
0          114688
             dsm         1912832              0
```

```
0         7176192
    f10appioserv          188416              0
0          139264
!----------------output truncated ------------------!
FTOS#
```

Example (stack-unit)

```
FTOS#show processes memory stack-unit 1
Total:  2147483648, MaxUsed:   401354752, CurrentUsed:
401354752, CurrentFree:  1746128896
    TaskName      TotalAllocated       TotalFreed
MaxHeld    CurrentHolding
    f10appioserv          188416              0
0          106496
           ndpm           630784              0
0         5255168
    f10appioserv          188416              0
0          139264
        mlagmgr           114688              0
0         4861952
    f10appioserv          188416              0
0          122880
           vrrp           323584              0
0         5451776
    f10appioserv          188416              0
0          139264
           frrp           184320              0
0         5042176
    f10appioserv          188416              0
0          118784
           xstp          4513792              0
0         9207808
    f10appioserv          188416              0
0          139264
            pim           950272              0
0         5345280
    f10appioserv          188416              0
0          139264
           igmp           499712              0
0         5365760
    f10appioserv          188416              0
0          118784
           mrtm          5943296              0
0        11030528
    f10appioserv          188416              0
0          106496
          l2mgr           950272              0
0        20856832
    f10appioserv          188416              0
0          139264
           l2pm           188416              0
0         5165056
    f10appioserv          188416              0
0          139264
!----------------output truncated ------------------!
FTOS#
```

Example (management-unit)

```
FTOS#show processes memory management-unit
Total      :  2147483648, MaxUsed    :   401399808 [04/30/2013
10:34:00]
CurrentUsed:   401399808, CurrentFree:  1746083840
SharedUsed :    14392520, SharedFree :     7627600
```

```
PID   Process            ResSize       Size       Allocs
Frees        Max       Current
400 ndpm                 5255168      630784
4848           0        4848        4848
328 mlagmgr              4861952      114688
0           0           0           0
351 vrrp                 5451776      323584
34008           0       34008       34008
445 frrp                 5042176      184320      153906
99384       87650       54522
345 xstp                 9207808     4513792
38510           0       38510       38510
117 pim                  5345280      950272
62168           0       62168       62168
241 igmp                 5365760      499712       19028
16564       18940        2464
429 mrtm               11030528     5943296
73110           0       73110       73110
425 l2mgr              20856832      950272      272526
149076      189706      123450
324 l2pm                 5165056      188416      303258
231896      137618       71362
219 arpm                 4796416      446464
38052           0       38052       38052
412 otm                  4927488      184320
968           0         968         968
371 dsm                  7176192     1912832    18890026
18767012      172706      123014
363 rtm                  6090752     1519616       62060
33128       62060       28932
349 rip                  4812800      212992
528           0         528         528
343 lacp                 4800512      233472
71984           0       71984       71984
332 ipm1                 5165056      659456
34184           0       34184       34184
319 acl                  5701632     1085440      107052
66256      107052       40796
FTOS#
```

show software ifm

Display interface management (IFM) data.

S5000

Syntax

`show software ifm {clients [summary] | ifagt` *`number`* `| ifcb` *`interface-type slot/port`* `| stack-unit` *`unit-number`* `| trace-flags}`

Parameters

clients	Enter the keyword `clients` to display IFM client information.
summary	(OPTIONAL) Enter the keyword `summary` to display brief information about IFM clients.
ifagt ***number***	Enter the keyword `ifagt` followed by the number of an interface agent to display software pipe and IPC statistics.

ifcb *interface-type slot/port*	Enter the keyword `ifcb` followed by the interface type and slot/port or number information. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0. • For a Null interface, enter the keywords `null 0`. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
stack-unit *unit-number*	Enter the keyword `stack-unit` followed by a number. The range is 0-11.
trace-flags	Enter the keyword `trace-flags` to display IFM information for internal trace flags.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show software ifm clients summary
ClntType  Inst     svcMask    subSvcMask   tlvSvcMask
tlvSubSvc swp
IPM       0      0x00000000 0x00000000 0x90ff71f3 0xb9878021 12
RTM       0      0x00000000 0x00000000 0x800010ff 0x0067c798 31
ISIS      0      0x00000002 0x00000000 0x00000000 0x00000000 0
VRRP      0      0x00000000 0x00000000 0x803330f3 0x0013c000 37
L2PM      0      0x00000000 0x00000000 0x87ff79ff 0xdb80c800 69
ACL       0      0x00000000 0x00000000 0x867f50c3 0x0103c018 78
PIM       0      0x000e00f3 0x0000c000 0x00000000 0x00000000 0
IGMP      0      0x000e027f 0x01000000 0x00000000 0x00000000 0
SNMP      0      0x00000000 0x00000000 0x800002c0 0x0000c002 13
EVTTERM   0      0x00000000 0x00000000 0x800002c0 0x0003c000 11
FEFD      0      0x00000000 0x00000000 0x8000300f 0x00000004 10
MRTM      0      0x00000000 0x00000000 0x81f7103f 0xc0600000 22
DSM       0      0x00000000 0x00000000 0x80771033 0x00000000 44
Mirror    0      0x00000000 0x00000000 0x80770003 0x00000000 15
LACP      0      0x00000000 0x00000000 0x8000383f 0x01000000 27
SFL_CP    0      0x00000000 0x00000000 0x807739ff 0x00000000 14
DHCP      0      0x00000000 0x00000000 0x807040f3 0x18001000 55
```

```
V6RAD     0      0x00000433 0x0000c000 0x00000000 0x00000000 0
Unidentified Client0 0x006e0002 0x00000000 0x00000000
0x00000000 0
LLDP      0      0x007f2433 0x0408c000 0x007f2433 0x0408c000 95
HYPERPULL 0      0x00000000 0x00000000 0x80001033 0x00100000 90
MLAGMGR   0      0x010683f0 0x01000000 0x60768030 0x01000000 40
FTOS#
```

show system

Display the current status of all stack members or a specific member.

S5000

Syntax `show system [brief | stack-unit unit-number]`

Parameters

brief	(OPTIONAL) Enter the keyword `brief` to view an abbreviated list of system information.
stack-unit ***unit-number***	(OPTIONAL) Enter the keyword `stack-unit` followed by a number. The range is 0 to 11.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#  show system

Stack MAC : 5c:f9:dd:ef:0a:c0
Reload-Type        :   normal-reload [Next boot : normal-
reload]

--  Unit 0 --
Unit Type       : Management Unit
Status          : online
Next Boot       : online
Required Type   : S5000 - 4-module, 4-port GE/TE/FG (SH)
Current Type    : S5000 - 4-module, 4-port GE/TE/FG (SH)
Master priority : 0
Hardware Rev    : 3.0
Num Ports       : 64
Up Time         : 46 min, 55 sec
FTOS Version    : 9.0(1.3)
Jumbo Capable   : yes
POE Capable     : no
FIPS Mode       : disabled
Burned In MAC   : 5c:f9:dd:ef:0a:c0
No Of MACs      : 64

--  Module 0 --
Status          : online
```

```
Module Type     : S5000-MOD-12xFC8ETH10-U - 12-port FC SFP+
(SH)
Num Ports       : 12
Hot Pluggable   : no

--  Module 1 --
Status          : online
Module Type     : S5000-MOD-12xETH10-F - 12-port 10GE SFP+ (SH)
Num Ports       : 12
Hot Pluggable   : no

--  Module 2 --
Status          : online
Module Type     : S5000-MOD-12xETH10-F - 12-port 10GE SFP+ (SH)
Num Ports       : 12
Hot Pluggable   : no

--  Module 3 --
Status          : online
Module Type     : S5000-MOD-12xETH10-F - 12-port 10GE SFP+ (SH)
Num Ports       : 12
Hot Pluggable   : no

--  Power Supplies  --
Unit   Bay   Status       Type    FanStatus
----------------------------------------------------------------
-------------
  0     0    up           AC      up
  0     1    up           AC      up

--  Fan  Status  --
Unit Bay   TrayStatus  Fan0    Speed   Fan1    Speed   Fan2
Speed   Fan3    Speed
----------------------------------------------------------------
-----------------------
0 absent or down
0    1         up       up      12000   up      12000
up      12000   up      12000
0    2         up       up      12000   up      12000
up      12000   up      12000
0 absent or down

Speed in RPM

--  Unit 1 --
Unit Type       : Member Unit
Status          : not present
Required Type   :      -

--  Unit 2 --
Unit Type       : Member Unit
Status          : not present
Required Type   :      -

--  Unit 3 --
Unit Type       : Member Unit
Status          : not present
Required Type   :      -

--  Unit 4 --
Unit Type       : Member Unit
Status          : not present
Required Type   :      -
```

```
--  Unit 5 --
Unit Type       : Member Unit
Status          : not present
Required Type   :      -

--  Unit 6 --
Unit Type       : Member Unit
Status          : not present
Required Type   :      -

--  Unit 7 --
Unit Type       : Member Unit
Status          : not present
Required Type   :      -

--  Unit 8 --
Unit Type       : Member Unit
Status          : not present
Required Type   :      -

--  Unit 9 --
Unit Type       : Member Unit
Status          : not present
Required Type   :      -

--  Unit 10 --
Unit Type       : Member Unit
Status          : not present
Required Type   :      -

--  Unit 11 --
Unit Type       : Member Unit
Status          : not present
Required Type   :      -

FTOS#
```

Example (brief)

```
FTOS#show system brief

Stack MAC : 5c:f9:dd:ee:ff:c0
Reload-Type        :   normal-reload [Next boot : normal-
reload]

--  Stack Info  --
Unit  UnitType    Status        ReqTyp CurTyp Version   Ports
--------------------------------------------------------------
  0   Management  online        S5000  S5000  1-0-0-45  64
  1   Member      not present
  2   Member      not present
  3   Member      not present
  4   Member      not present
  5   Member      not present
  6   Member      not present
  7   Member      not present
  8   Member      not present
  9   Member      not present
 10   Member      not present
 11   Member      not present

--  Power Supplies  --
Unit   Bay   Status  Type  FanStatus
-----------------------------------------------------------
Unit   Bay   Status  Type  FanStatus
```

```
----------------------------------------------------------
  0     0    up      AC      up
  0     1    up      AC      up

--  Fan  Status  --
Unit Bay Tray  Fan0 Speed Fan1 Speed Fan2 Speed Fan3 Speed
         Status
----------------------------------------------------------
 0   0  absent or down
 0   1  up    up   7200  up   7200  up   7200  up   7200
 0   2  up    up   7200  up   7200  up   7200  up   7200
 0   3     absent or down

Speed in RPM

FTOS#
```

Example (stack-unit)

```
FTOS#show system stack-unit 1

--  Unit 1 --
Unit Type        : Management Unit
Status           : online
Next Boot        : online
Required Type    : S5000 - 4-module, 4-port GE/TE/FG (SH)
Current Type     : S5000 - 4-module, 4-port GE/TE/FG (SH)
Master priority : 14
Hardware Rev     : 1.0
Num Ports        : 64
Up Time          : 5 day, 17 hr, 10 min
FTOS Version     : 9.0(1.3)
Jumbo Capable    : yes
POE Capable      : no
FIPS Mode        : disabled
Boot Flash       : A: 1.3.1.1p  [booted]   B: 1.3.1.1p
Boot Selector    : 1.3.0.0m
Memory Size      : 2147483648 bytes
Serial Number    : NA
Part Number      : 7520068201 Rev C
Vendor Id        : NA
Date Code        : NA
Country Code     : NA
Piece Part ID    : FX128U00014
PPID Revision    : A00
Service Tag      : INVALID
Expr Svc Code    : NA
Auto Reboot      : disabled
Burned In MAC    : 5c:f9:dd:ef:02:00
No Of MACs       : 64

--  Module 0 --
Status           : online
Module Type      : S5000-MOD-12xETH10-F - 12-port 10GE SFP+ (SH)
Num Ports        : 12
Hot Pluggable    : no

--  Module 1 --
Status           : not present

--  Module 2 --
Status           : not present

--  Module 3 --
Status           : not present
```

```
--  Power Supplies  --
Unit   Bay   Status       Type    FanStatus
---------------------------------------------------------------
-------------
  1     0    up           AC      up
  1     1    up           AC      up

--  Fan  Status  --
Unit Bay   TrayStatus  Fan0    Speed   Fan1    Speed   Fan2
Speed   Fan3    Speed
---------------------------------------------------------------
-----------------------
1      absent or down
1    1     up          up      12000   up      12000   up
12000   up      12000
1    2     up          up      12000   up      12000   up
12000   up      12000
1      absent or down

Speed in RPM

FTOS#
```

Related Commands

show version – displays the FTOS version.

show processes memory – displays memory usage based on running processes.

show hardware stack-unit – displays the data plane and management plane input and output statistics of a particular stack member.

show tech-support

Display a collection of data from other show commands, necessary for Dell Networking technical support to perform troubleshooting on S5000 switches.

S5000

Syntax

`show tech-support [stack-unit unit-number | page]`

Parameters

stack-unit *unit-number*	(OPTIONAL) Enter the keyword `stack-unit` followed by a number. The range is 0 to 11.
page	(OPTIONAL) Enter the keyword `page` to view 24 lines of text at a time. Press the SPACE BAR to view the next 24 lines. Press ENTER to view the next line of text. When using the pipe command (|), enter one of these keywords to filter command output. For details about filtering commands, refer to CLI Basics.
save	Enter the keyword `save` to save the command output. flash: Save to local flash drive (`flash://filename` [max 20 chars]).

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Without the `page` or `stack-unit` option, the command output is continuous. Use Ctrl-z to interrupt the command output.

The `save` option works with other filtering commands. This allows you to save specific information of a `show` command. The `save` entry must always be the last option. For example:

```
FTOS#show tech-support |grep regular-expression |except
regular-expression | find regular-expression | save flash://
result
```

This display output is an accumulation of the same information that is displayed when you execute one of the following show commands:

- `show cam`
- `show clock`
- `show environment`
- `show file`
- `show interfaces`
- `show inventory`
- `show ip protocols`
- `show ip route summary`
- `show processes cpu`
- `show processes memory`
- `show redundancy`
- `show running-conf`
- `show version`

Example (save)

```
FTOS#show tech-support ?

page       Page through output
stack-unit Unit Number
|          Pipe through a command
<cr>

FTOS#show tech-support stack-unit 1 ?
|          Pipe through a command
<cr>

FTOS#show tech-support stack-unit 1 | ?
except                  Show only text that does not match a
pattern
find                    Search for the first occurrence of a
pattern
grep                    Show only text that matches a pattern
no-more                 Don't paginate output
save                    Save output to a file
FTOS#

FTOS#show tech-support stack-unit 1 | save ?
flash:                  Save to local file system (flash://
filename (max 20 chars) )
usbflash:               Save to local file system (usbflash://
filename (max 20 chars) )
FTOS#

FTOS#show tech-support stack-unit 1 | save flash://ShowSave
Start saving show command report .......

FTOS#
FTOS#dir
Directory of flash:

  1  drwx       4096   Jan 01 1980 00:00:00 +00:00 .
  2  drwx       2048   Apr 24 2013 17:26:56 +00:00 ..
  3  drwx       4096   Jan 01 1970 00:00:00 +00:00
TRACE_LOG_DIR
  4  drwx       4096   Jan 01 1970 00:00:00 +00:00
CORE_DUMP_DIR
  5  d---       4096   Jan 01 1970 00:00:00 +00:00 ADMIN_DIR
  6  drwx       4096   Jan 01 1970 00:00:00 +00:00
RUNTIME_PATCH_DIR
  7  -rwx       6166   Jan 24 2013 03:50:10 +00:00 mani_ecmp2
  8  drwx       4096   Apr 18 2013 18:41:50 +00:00
CONFIG_TEMPLATE
  9  -rwx       6383   Feb 01 2013 02:15:42 +00:00 str
10  -rwx       3659   Apr 05 2013 00:32:58 +00:00 startup-
config
11  -rwx         69   Nov 27 2012 16:48:40 +00:00 TestReport-
SU-0.txt
12  -rwx       3755   Nov 13 2012 11:22:08 +00:00 pt5diablo.txt
13  -rwx   61824995   Jan 13 2013 13:19:44 +00:00 abc1
14  -rwx         69   Nov 28 2012 17:15:20 +00:00
backup_diag_results.txt
15  -rwx       4442   Jan 06 2013 16:29:24 +00:00 pt-s5000-
startupconfig
16  -rwx       5075   Jan 12 2013 15:51:18 +00:00
pt5_vlt_tor.txt
17  -rwx   61752428   Jan 13 2013 13:20:20 +00:00 abc2
18  -rwx       6624   Feb 13 2013 11:04:28 +00:00 pt5_stack.txt
19  -rwx       5950   Jan 22 2013 00:00:46 +00:00 mani
20  -rwx       6361   Jan 22 2013 09:10:38 +00:00 mani_ecmp
21  -rwx       6383   Jan 24 2013 00:27:22 +00:00 mani_ecmp1
22  -rwx       7503   Feb 22 2013 13:52:24 +00:00 mani.cfg
23  -rwx   50066729   Jan 29 2013 16:11:44 +00:00 SMARTSCRIPTS.
1.1.1.tar.gz
24  -rwx       7987   Mar 05 2013 17:36:38 +00:00 debug.cfg
25  -rwx       8376   Mar 05 2013 17:11:28 +00:00 backup-
march-4-kp.cfg
26  -rwx       8930   Mar 09 2013 16:01:18 +00:00 startup-
config.bak
27  -rwx       6196   Feb 21 2013 00:23:36 +00:00
dhcpBindConflict
28  -rwx       8162   Feb 22 2013 02:33:38 +00:00 mani_link

flash: 2143281152 bytes total (1482190848 bytes free)
FTOS#
```

Example

```
FTOS#show tech-support stack-unit 0
---------- show version -------------------
Dell Force10 Real Time Operating System Software
Dell Force10 Operating System Version: 2.0
Dell Force10 Application Software Version: 9.0(1.3)
Fiber Channel Firmware Version: V10.1.0.00.04
Copyright (c) 1999-2013 by Dell Inc. All Rights Reserved.
Build Time: Thu Apr 18 11:12:20 PDT 2013
Build Path: /sites/sjc/work/build/buildSpaces/build12/
E9-0-1/SW/SRC
FTOS uptime is 5 day(s), 17 hour(s), 19 minute(s)

System image file is "lnaidu-dcb"

System Type: S5000
Control Processor: Freescale QorIQ P2020 with 2147483648 bytes
of memory.

16M bytes of boot flash memory.

  1 4-module, 4-port GE/TE/FG (SH)
12 Ten GigabitEthernet/IEEE 802.3 interface(s)
  4 Forty GigabitEthernet/IEEE 802.3 interface(s)

----------- show clock ----------------------
10:46:02.545 UTC Tue Apr 30 2013

----------- show running-config --------------
FTOS#show running-config
Current Configuration ...
! Version 9.0(1.3)
! Last configuration change at Tue Apr 30 10:12:51 2013 by
admin
!
boot system stack-unit 1 primary tftp://10.11.8.12/lnaidu-dcb
boot system stack-unit 1 secondary tftp://10.11.8.13/FTOS-
SH-1-0-0-270.bin
boot system stack-unit 1 default tftp://10.11.8.13/FTOS-
SH-1-0-0-270.bin
boot system gateway 10.11.227.254
!
redundancy auto-synchronize full
redundancy disable-auto-reboot stack-unit
!
redundancy disable-auto-reboot stack-unit 0
redundancy disable-auto-reboot stack-unit 1
redundancy disable-auto-reboot stack-unit 2
redundancy disable-auto-reboot stack-unit 3
redundancy disable-auto-reboot stack-unit 4
redundancy disable-auto-reboot stack-unit 5
redundancy disable-auto-reboot stack-unit 6
redundancy disable-auto-reboot stack-unit 7
redundancy disable-auto-reboot stack-unit 8
redundancy disable-auto-reboot stack-unit 9
redundancy disable-auto-reboot stack-unit 10
redundancy disable-auto-reboot stack-unit 11!
!--------output truncated ---------!
```

Related Commands

show version – displays the FTOS version.

show system – displays the current switch status.

show environment – displays the system component status.

show processes memory – displays memory usage based on running processes.

telnet

Connect through Telnet to a server. The Telnet client and server in FTOS support IPv4 and IPv6 connections.

You can establish a Telnet session directly to the router or a connection can be initiated from the router.

S5000

Syntax

`telnet {host | ip-address | ipv6-address | word /source-interface}`

Parameters

host	Enter the name of a server.
ip-address	Enter the IPv4 address in dotted decimal format of the server.
ipv6-address	Enter the IPv6 address in the x:x:x:x::x format in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros. Only one occurrence of this notation is permitted in an IPv6 address.
word **/source-interface**	(OPTIONAL) Enter a word followed by the `/source interface` keyword, then enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults

Not configured.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Telnet to link-local addresses is not supported.

terminal length

Configure the number of lines displayed on the terminal screen.

S5000

Syntax

```
terminal length screen-length
```

Parameters

screen-length	Enter a number of lines. Entering zero causes the terminal to display without pausing. The range is 0 to 512.

Defaults 24 lines

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

traceroute

View a packet's path to a specific device.

S5000

Syntax

```
traceroute {host | ip-address | ipv6-address | outgoing-
interface}
```

Parameters

host	Enter the name of device.
ip-address	Enter the IP address of the device in dotted decimal format.
ipv6-address	Enter the IPv6 address, in the x:x:x:x::x format, to which you are testing connectivity. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros. Only one occurrence of this notation is permitted in an IPv6 address.
outgoing-interface	(IPv6 link-local address) Enter one of the following interface types and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

- For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults

- Timeout = **5 seconds**
- Probe count = **3**
- 30 hops max
- 40 byte packet size
- UDP port = **33434**

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you enter the `traceroute` command without specifying an IP address (Extended Traceroute), you are prompted for a target and source IP address, timeout (in seconds) (default is **5**), a probe count (default is **3**), minimum TTL (default is **1**), maximum TTL (default is **30**), and port number (default is **33434**). To keep the default setting for those parameters, press the ENTER key.

For the `source IP address` option, you may enter IPv6 global addresses only (link-local addresses are not supported).

For IPv6, you are prompted for a minimum hop count (default is **1**) and a maximum hop count (default is **64**).

Example (name)

```
FTOS#traceroute www.dell.com

Translating "www.dell.com"...domain server (10.11.0.1) [OK]
Type Ctrl-C to abort.

------------------------------------------------------------
Tracing the route to www.dell.com (10.11.84.18),
30 hops max, 40 byte packets
------------------------------------------------------------

TTL Hostname            Probe1       Probe2       Probe3
1   10.11.199.190   001.000 ms   001.000 ms   002.000 ms
2   gwegress-sjc-02.dell.com (10.11.30.126) 005.000 ms 001.000
ms 001.000 ms
3   fw-sjc-01.dell.com (10.11.127.254) 000.000 ms 000.000 ms
000.000 ms
4   www.dell.com (10.11.84.18) 000.000 ms 000.000 ms 000.000 ms
FTOS#
```

Example (IPv4)

```
FTOS#traceroute 10.1.1.1

Type Ctrl-C to abort.
```

```
----------------------------------------------------------------
Tracing the route to 10.11.197.31, 30 hops max, 40 byte packets
----------------------------------------------------------------
 TTL Hostname         Probe1      Probe2      Probe3
  1  10.1.1.1     0000000 ms  0000000 ms  0000000 ms
FTOS#
```

Example (IPv6)

```
FTOS#traceroute 100::1

Type Ctrl-C to abort.

----------------------------------------------------------
Tracing the route to 100::1, 64 hops max, 60 byte packets
----------------------------------------------------------
Hops Hostname       Probe1      Probe2      Probe3
1    100::1     000.000 ms  000.000 ms  000.000 ms

FTOS#traceroute 3ffe:501:ffff:100:201:e8ff:fe00:4c8b

Type Ctrl-C to abort.

-----------------------------------------------------------
Tracing the route to 3ffe:501:ffff:100:201:e8ff:fe00:4c8b,
64 hops max, 60 byte packets
-----------------------------------------------------------
Hops Hostname    Probe1       Probe2       Probe3
 1   3ffe:501:ffff:100:201:e8ff:fe00:4c8b
             000.000 ms   000.000 ms   000.000 ms
FTOS#
```

Related Commands

ping – tests the connectivity to a device.

undebug all

Disable all debug operations on the system.

S5000

Syntax `undebug all`

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

write

Copy the current configuration to either the startup-configuration file or the terminal.

S5000

Syntax `write {memory | terminal}`

Parameters

memory	Enter the keyword `memory` to copy the current running configuration to the startup configuration file. This command is similar to the `copy running-config startup-config` command.
terminal	Enter the keyword `terminal` to copy the current running configuration to the terminal. This command is similar to the `show running-config` command.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The `write memory` command saves the running-configuration to the file labeled startup-configuration. When using a LOCAL CONFIG FILE other than the startup-config not named "startup-configuration" (for example, you used a specific file during the `boot config` command), the running-config is not saved to that file; use the `copy` command to save any running-configuration changes to that local file.

Related Commands save – saves configurations created in BOOT_USER mode (BLI).

5

802.1ag

802.1ag issupported on the S5000 switch.

ccm disable

Disable continuity check message (CCM).

S5000

Syntax `ccm disable`

Enter `no ccm disable` to enable CCM.

Defaults Disabled

Command Modes ECFM DOMAIN

Command History

Version 9.0(1.3)	Introduced on the S5000.

ccm transmit-interval

Configure the transmit interval (mandatory). The interval specified applies to all maintenance endpoints (MEPs) in the domain.

S5000

Syntax `ccm transmit-interval` *`seconds`*

Parameters

seconds	Enter a transmit interval. The range is 1, 10, 60, and 600.

Defaults 10 seconds

Command Modes ECFM DOMAIN

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ethernet cfm traceroute-cache

Delete all link trace cache entries.

S5000

Syntax	`clear ethernet cfm traceroute-cache`
Defaults	none
Command Modes	ECFM DOMAIN
Command History	**Version 9.0(1.3)** Introduced on the S5000.

database hold-time

Set the amount of time that data from a missing MEP is kept in the continuity check database.

S5000

Syntax	`database hold-time` *`minutes`*
Parameters	***minutes*** Enter a hold-time. The range is 100 to 65535 minutes.
Defaults	**100 minutes**
Command Modes	ECFM DOMAIN
Command History	**Version 9.0(1.3)** Introduced on the S5000.

disable

Disable Ethernet CFM without stopping the CFM process.

S5000

Syntax	`disable`
Defaults	Disabled
Command Modes	ETHERNET CFM
Command History	**Version 9.0(1.3)** Introduced on the S5000.

domain

Create the maintenance domain.

S5000

Syntax domain *name* md-level *number*

Parameters

name	Name the maintenance domain.
md-level *number*	Enter a maintenance domain level. The range is 0 to 7.

Defaults none

Command Modes ETHERNET CFM

Command History

Version 9.0(1.3)	Introduced on the S5000.

ethernet cfm

Spawn the CFM process. No CFM configuration is allowed until the CFM process is spawned.

S5000

Syntax ethernet cfm

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

ethernet cfm mep

Create an MEP.

S5000

Syntax ethernet cfm mep {up-mep | down-mep} domain {*name* | *level*} ma-name *name* mepid *mep-id*

Parameters

[up-mep | down-mep]	Specify whether the MEP is up or down facing. • Up-MEP: monitors the forwarding path internal to a bridge on the customer or provider edge; on Dell Networking switches,

the internal forwarding path is effectively the switch fabric and forwarding engine.

- Down-MEP: monitors the forwarding path external to another bridge.

domain [*name* | *level*]	Enter the keyword `domain` and then enter the domain name or domain level.
ma-name *name*	Enter the keyword `ma-name` and then enter the name of the maintenance association.
mepid *mep-id*	Enter an MEP ID. The range is 1 to 8191.

Defaults none

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

ethernet cfm mip

Create a maintenance intermediate point (MIP).

S5000

Syntax `ethernet cfm mip domain {name | level} ma-name name`

Parameters

domain [*name* | *level*]	Enter the keyword `domain` and then enter the domain name or domain level.
ma-name *name*	Enter the keyword `ma-name` and then enter the name of the maintenance association.

Defaults none

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

mep cross-check

Enable cross-checking for a MEP.

S5000

Syntax `mep cross-check mep-id`

Parameters

mep-id	Enter the MEP ID. The range is 1 to 8191.

Defaults none

Command Modes ECFM DOMAIN

Command History

Version 9.0(1.3)	Introduced on the S5000.

mep cross-check enable

Enable cross-checking.

S5000

Syntax `mep cross-check enable {port | vlan-id}`

Parameters

port	Down service with no VLAN association.
vlan-id	Enter the VLAN to apply the cross-check.

Defaults none

Command Modes ECFM DOMAIN

Command History

Version 9.0(1.3)	Introduced on the S5000.

mep cross-check start-delay

Configure the amount of time the system waits for a remote MEP to come up before the cross-check operation is started.

S5000

Syntax `mep cross-check start-delay number`

Parameters

start-delay ***number***	Enter a start-delay in seconds. The range is 3 to 100 seconds.

Defaults **3 ccms**

Command Modes ETHERNET CFM

Command History

Version 9.0(1.3)	Introduced on the S5000.

ping ethernet

Send a loopback message.

S5000

Syntax

```
ping ethernet domain [name l level] ma-name ma-name remote
{dest-mep-id | mac-addr mac-address} source {src-mep-id | port
interface}
```

Parameters

name* | *level	Enter the domain name or level.
ma-name ***ma-name***	Enter the keyword `ma-name` and then enter the maintenance association name.
dest-mep-id	Enter the MEP ID that is the target of the ping.
mac-addr ***mac-address***	Enter the keyword `mac-addr` and then enter the MAC address that is the target of the ping.
src-mep-id	Enter the MEP ID that originates the ping.
port ***interface***	Enter the keyword `port` and then enter the interface that originates the ping.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

service

Create maintenance association.

S5000

Syntax `service name vlan vlan-id`

Parameters

name	Enter a maintenance association name.
vlan *vlan-id*	Enter the keyword `vlan` and then enter the VLAN ID. The range is 1 to 4094.

Defaults none

Command Modes ECFM DOMAIN

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ethernet cfm domain

Display maintenance domain information.

S5000

Syntax `show ethernet cfm domain [name | level | brief]`

Parameters

name* | *level	Enter the maintenance domain name or level.
brief	Enter the keyword `brief` to display a summary output.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS# show ethernet cfm domain
Domain Name: customer
Level: 7
Total Service: 1
   Services
      MA-Name     VLAN         CC-Int         X-CHK Status
      My_MA         200          10s            enabled
Domain Name: My_Domain
Level: 6
Total Service: 1
   Services
```

```
MA-Name      VLAN         CC-Int         X-CHK Status
Your_MA      100         10s             enabled
```

show ethernet cfm maintenance-points local

Display configured MEPs and MIPs.

S5000

Syntax `show ethernet cfm maintenance-points local [mep | mip]`

Parameters

mep	Enter the keyword `mep` to display configured MEPs.
mip	Enter the keyword `mip` to display configured MIPs.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ethernet cfm maintenance-points local mip
-----------------------------------------------------
MPID Domain Name Level  Type Port CCM-Status
     MA Name     VLAN   Dir  MAC
-----------------------------------------------------
0 service1       4     MIP  Te 0/5    Disabled
  My_MA        3333    DOWN 00:01:e8:0b:c6:36

0 service1       4     MIP  Te 0/5    Disabled
  Your_MA      3333    UP   00:01:e8:0b:c6:36
```

show ethernet cfm maintenance-points remote

Display the MEP Database.

S5000

Syntax

```
show ethernet cfm maintenance-points remote detail [active |
domain {level | name} | expired | waiting]
```

Parameters

active	Enter the keyword `active` to display only the MEPs in active state.
domain [*name* | *level*]	Enter the keyword `domain` and then enter the domain name or domain level.

expired	Enter the keyword `expired` to view MEP entries that have expired due to connectivity failure.
waiting	Enter the keyword `waiting` to display MEP entries waiting for response.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ethernet cfm maintenance-points remote detail
MAC Address: 00:01:e8:58:68:78
Domain Name: cfm0
MA Name: test0
Level: 7
VLAN: 10
MP ID: 900
Sender Chassis ID: Dell
MEP Interface status: Up
MEP Port status: Forwarding
Receive RDI: FALSE
MP Status: Active
```

show ethernet cfm mipbd

Display the MIP database.

S5000

Syntax `show ethernet cfm mipdb`

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ethernet cfm port-statistics

Display CFM statistics by port.

S5000

Syntax `show ethernet cfm port-statistics [`*`interface type slot/port`*`]`

Parameters

interface *type*	Enter the keyword `interface` and then enter the interface type.
slot/port	Enter the slot and port numbers for the port.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ethernet cfm port-statistics interface
tengigabitethernet 0/5
Port statistics for port: Te 0/5
==================================
RX Statistics
=============
Total CFM Pkts 75394 CCM Pkts 75394
LBM Pkts 0 LTM Pkts 0
LBR Pkts 0 LTR Pkts 0
Bad CFM Pkts 0 CFM Pkts Discarded 0
CFM Pkts forwarded 102417
TX Statistics
=============
Total CFM Pkts 10303 CCM Pkts 0
LBM Pkts 0 LTM Pkts 3
LBR Pkts 0 LTR Pkts 0
```

show ethernet cfm statistics

Display MEP statistics.

S5000

Syntax `show ethernet cfm statistics [domain {`*`name`*` | `*`level`*`} vlan-id `*`vlan-id`*` mpid `*`mpid`*`]`

Parameters

domain	Enter the keyword `domain` to display statistics for a particular domain.
name* | *level	Enter the domain name or level.
vlan-id *vlan-id*	Enter the keyword `vlan-id` and then enter a VLAN ID.
mpid *mpid*	Enter the keyword `mpid` and then enter a maintenance point ID.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS# show ethernet cfm statistics
Domain Name: Customer
Domain Level: 7
MA Name: My_MA
MPID: 300

 CCMs:
  Transmitted:          1503   RcvdSeqErrors: 0
 LTRs:
  Unexpected Rcvd:      0
 LBRs:
  Received:             0      Rcvd Out Of Order: 0
  Received Bad MSDU:    0
  Transmitted:          0
```

show ethernet cfm traceroute-cache

Display the link trace cache.

S5000

Syntax

```
show ethernet cfm traceroute-cache
```

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ethernet cfm traceroute-cache

Traceroute to 00:01:e8:52:4a:f8 on Domain Customer2, Level 7,
MA name Test2 with VLAN
2
------------------------------------------------------
Hops     Host              IngressMAC         Ingr Action
Relay Action
       Next Host           Egress MAC         Egress Action
FWD Status
--------------------------------------------------------
4  00:00:00:01:e8:53:4a:f8  00:01:e8:52:4a:f8   IngOK
RlyHit
   00:00:00:01:e8:52:4a:f8
Terminal MEP
```

traceroute cache hold-time

Set the amount of time a trace result is cached.

S5000

Syntax	`traceroute cache hold-time` *`minutes`*
Parameters	*minutes* — Enter a hold-time. The range is 10 to 65535 minutes.
Defaults	100 minutes
Command Modes	ETHERNET CFM
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

traceroute cache size

Set the size of the link trace cache.

S5000

Syntax	`traceroute cache size` *`entries`*
Parameters	*entries* — Enter the number of entries the link trace cache can hold. The range is 1 to 4095 entries.
Defaults	100 entries
Command Modes	ETHERNET CFM
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

traceroute ethernet

Send a linktrace message to an MEP.

S5000

Syntax

```
traceroute ethernet domain [name | level] ma-name remote {mep-id mep-id | mac-addr mac-address}
```

Parameters

domain *name* | *level*	Enter the keyword `domain` and then enter the domain name or level.
ma-name *ma-name*	Enter the keyword `ma-name` and then enter the maintenance association name.
mepid *mep-id*	Enter the MEP ID that is the trace target.
mac-addr *mac-address*	Enter the MAC address of the trace target.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

6

802.1X

An authentication server must authenticate a client connected to an 802.1X switch port. Until the authentication, only extensible authentication protocol over LAN (EAPOL) traffic is allowed through the port to which a client is connected. After authentication is successful, normal traffic passes through the port.

FTOS supports remote authentication dial-in service (RADIUS) and active directory environments using 802.1X Port Authentication.

Important Points to Remember

FTOS limits network access for certain users by using virtual local area network (VLAN) assignments. 802.1X with VLAN assignment has these characteristics when configured on the switch and the RADIUS server.

- 802.1X is supported on the S5000.
- On all platforms, if the primary RADIUS server becomes unresponsive, the authenticator begins using a secondary RADIUS server, if configured.
- If no VLAN is supplied by the RADIUS server or if you disable 802.1X authorization, the port configures its access VLAN after successful authentication.
- If you enable 802.1X authorization but the VLAN information from the RADIUS server is not valid, the port returns to the Unauthorized state and remains in the configured access VLAN. This safeguard prevents ports from appearing unexpectedly in an inappropriate VLAN due to a configuration error. Configuration errors create an entry in Syslog.
- If you enable 802.1X authorization and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.
- If you enable port security on an 802.1X port with VLAN assignment, the port is placed in the RADIUS server assigned VLAN.
- If you disable 802.1X on the port, it returns to the configured access VLAN.
- When the port is in the Force Authorized, Force Unauthorized, or Shutdown state, it is placed in the configured access VLAN.
- If an 802.1X port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration does not take effect.
- The 802.1X with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN membership.

debug dot1x

Display 802.1X debugging information.

S5000

Syntax

```
debug dot1x [all | auth-pae-fsm | backend-fsm | eapol-pdu]
[interface interface]
```

Parameters

all	Enable all 802.1X debug messages.
auth-pae-fsm	Enable authentication PAE FSM debug messages.
backend-fsm	Enable backend FSM debug messages.
eapol-pdu	Enable the EAPOL frame trace and related debug messages.
interface *interface*	Restricts the debugging information to an interface.

Defaults Disabled

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

dot1x auth-fail-vlan

Configure an authentication failure VLAN for users and devices that fail 802.1X authentication.

S5000

Syntax

```
dot1x auth-fail-vlan vlan-id [max-attempts number]
```

To delete the authentication failure VLAN, use the `no dot1x auth-fail-vlan vlan-id [max-attempts number]` command.

Parameters

vlan-id	Enter the VLAN Identifier. The range is 1 to 4094.
max-attempts *number*	(OPTIONAL) Enter the keywords `max-attempts` followed number of attempts desired before authentication fails. The range is 1 to 5. The default is **3**.

Defaults **3** attempts

Command Modes CONFIGURATION (*conf-if-interface-slot/port*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	If the host responds to 802.1X with an incorrect login/password, the login fails. The switch attempts to authenticate again until the maximum attempts configured is reached. If the authentication fails after all allowed attempts, the interface moves to the authentication failed VLAN. After the authentication VLAN is assigned, the port-state must be toggled to restart authentication. Authentication occurs at the next reauthentication interval (`dot1x reauthentication`).
Related Commands	• dot1x port-control • dot1x guest-vlan • show dot1x interface

dot1x auth-server

Configure the authentication server to RADIUS.

S5000

Syntax	`dot1x auth-server radius`
Defaults	none
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.

dot1x auth-type mab-only

Use only the host MAC address to authenticate a device with MAC authentication bypass (MAB).

S5000

Syntax	`dot1x auth-type mab-only`
Defaults	Disabled
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	The prerequisites for enabling MAB-only authentication on a port are: • Enable 802.1X authentication globally on the switch and on the port (the `dot1x authentication` command).

- Enable MAC authentication bypass on the port (the `dot1x mac-auth-bypass` command).

In MAB-only authentication mode, a port authenticates using the host MAC address even though 802.1xauthentication is enabled. If the MAB-only authentication fails, the host is placed in the guest VLAN (if configured).

To disable MAB-only authentication on a port, enter the `no dot1x auth-type mab-only` command.

Related Commands dot1x mac-auth-bypass

dot1x authentication (Configuration)

Enable dot1x globally. Enable dot1x both globally and at the interface level.

S5000

Syntax `dot1x authentication`

To disable dot1x on a globally, use the `no dot1x authentication` command.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands dot1x authentication (Interface)

dot1x authentication (Interface)

Enable dot1x on an interface. Enable dot1x both globally and at the interface level.

S5000

Syntax `dot1x authentication`

To disable dot1x on an interface, use the `no dot1x authentication` command.

Defaults Disabled

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

dot1x authentication (Configuration)

dot1x guest-vlan

Configure a guest VLAN for limited access users or for devices that are not 802.1X capable.

S5000

Syntax

`dot1x guest-vlan` *`vlan-id`*

To disable the guest VLAN, use the `no dot1x guest-vlan` *`vlan-id`* command.

Parameters

vlan-id	Enter the VLAN Identifier. The range is 1 to 4094.

Defaults

Not configured.

Command Modes

CONFIGURATION (*conf-if-interface-slot/port*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

1X authentication is enabled when an interface is connected to the switch. If the host fails to respond within a designated amount of time, the authenticator places the port in the guest VLAN.

If a device does not respond within 30 seconds, it is assumed that the device is not 802.1X capable. Therefore, a guest VLAN is allocated to the interface, and authentication for the device occurs at the next reauthentication interval (`dot1x reauthentication`).

If the host fails authentication for the designated number of times, the authenticator places the port in authentication failed VLAN (`dot1x auth-fail-vlan`).

NOTE: You can create the Layer 3 portion of a guest VLAN and authentication fail VLANs whether the VLAN is assigned to an interface or not. After an interface is assigned a guest VLAN (which has an IP address), routing through the guest VLAN is the same as any other traffic. However, the interface may join/leave a VLAN dynamically.

Related Commands

- dot1x auth-fail-vlan
- dot1x reauthentication
- dot1x reauth-max
- show dot1x interface

dot1x host-mode

Enable single-host or multi-host authentication.

S5000

Syntax

```
dot1x host-mode {single-host | multi-host | multi-auth}
```

Parameters

single-host	Enable single-host authentication.
multi-host	Enable multi-host authentication.
multi-auth	Enable multi-supplicant authentication.

Defaults single-host

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

- Single-host mode authenticates only one host per authenticator port and drops all other traffic on the port.
- Multi-host mode authenticates the first host to respond to an Identity Request and then permits all other traffic on the port.
- Multi-supplicant mode authenticates every device attempting to connect to the network on the authenticator port.

Related Commands show dot1x interface

dot1x mac-auth-bypass

Enable MAC authentication bypass. If 802.1X times out because the host did not respond to the Identity Request frame, FTOS attempts to authenticate the host based on its MAC address.

S5000

Syntax

```
dot1x mac-auth-bypass
```

To disable MAC authentication bypass on a port, use the `no dot1x mac-auth-bypass` command.

Defaults Disabled

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands	dot1x auth-type mab-only

dot1x max-eap-req

Configure the maximum number of times an extensive authentication protocol (EAP) request is transmitted before the session times out.

S5000

Syntax

```
dot1x max-eap-req number
```

To return to the default, use the `no dot1x max-eap-req` command.

Parameters

number	Enter the number of times an EAP request is transmitted before a session time-out. The range is 1 to 10. The default is **2**.

Defaults 2

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

dot1x max-supplicants

Restrict the number of supplicants that can be authenticated and permitted to access the network through the port. This configuration is only takes effect in Multi-Auth mode.

S5000

Syntax

```
dot1x max-supplicants number
```

Parameters

number	Enter the number of supplicants that can be authenticated on a single port in Multi-Auth mode. The range is 1 to 128. The default is **128**.

Defaults 128 hosts can be authenticated on a single authenticator port.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands	dot1x host-mode

dot1x port-control

Enable port control on an interface.

S5000

Syntax `dot1x port-control {force-authorized | auto | force-unauthorized}`

Parameters

force-authorized	Enter the keywords `force-authorized` to forcibly authorize a port.
auto	Enter the keyword `auto` to authorize a port based on the 802.1X operation result.
force-unauthorized	Enter the keywords `force-unauthorized` to forcibly deauthorize a port.

Defaults none

Command Modes Auto

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The authenticator completes authentication only when `port-control` is set to `auto`.

dot1x quiet-period

Set the number of seconds that the authenticator remains quiet after a failed authentication with a client.

S5000

Syntax `dot1x quiet-period` *`seconds`*

To disable quiet time, use the `no dot1x quiet-time` command.

Parameters

seconds	Enter the number of seconds. The range is 1 to 65535. The default is **60**.

Defaults **60** seconds

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

dot1x reauthentication

Enable periodic reauthentication of the client.

S5000

Syntax	`dot1x reauthentication [interval seconds]` To disable periodic reauthentication, use the `no dot1x reauthentication` command.
Parameters	**interval *seconds*** — (Optional) Enter the keyword `interval` followed by the interval time, in seconds, after which reauthentication is initiated. The range is 1 to 31536000 (one year). The default is **3600** (1 hour).
Defaults	**3600** seconds (1 hour)
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

dot1x reauth-max

Configure the maximum number of times a port can reauthenticate before the port becomes unauthorized.

S5000

Syntax	`dot1x reauth-max number` To return to the default, use the `no dot1x reauth-max` command.
Parameters	***number*** — Enter the permitted number of reauthentications. The range is 1 to 10. The default is **2**.
Defaults	**2**
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

dot1x server-timeout

Configure the amount of time after which exchanges with the server time-out.

S5000

Syntax

`dot1x server-timeout` *`seconds`*

To return to the default, use the `no dot1x server-timeout` command.

Parameters

seconds	Enter a time-out value in seconds. The range is 1 to 300, where 300 is implementation dependant. The default is **30**.

Defaults

30 seconds

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you configure the `dot1x server-timeout` value, take into account the communication medium used to communicate with an authentication server and the number of RADIUS servers configured. Ideally, the `dot1x server-timeout` value (in seconds) is based on the configured RADIUS-server timeout and retransmit values and calculated according to the following formula: `dot1x server-timeout` *seconds* > (radius-server retransmit *seconds* + 1) * radius-server timeout *seconds*.

Where the default values are as follows: `dot1x server-timeout` (30 seconds), radius-server retransmit (3 seconds), and radius-server timeout (5 seconds).

For example:

```
FTOS(conf)#radius-server host 10.11.197.105 timeout 6
FTOS(conf)#radius-server host 10.11.197.105 retransmit 4
FTOS(conf)#interface tengigabitethernet 2/23
FTOS(conf-if-te-2/23)#dot1x server-timeout 40
```

dot1x supplicant-timeout

Configure the amount of time after which exchanges with the supplicant time-out.

S5000

Syntax

`dot1x supplicant-timeout` *`seconds`*

To return to the default, use the `no dot1x supplicant-timeout` command.

Parameters

seconds	Enter a time-out value in seconds. The range is 1 to 300, where 300 is implementation dependant. The default is **30**.

Defaults	**30** seconds
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

dot1x tx-period

Configure the intervals at which EAPOL PDUs the Authenticator PAE transmits.

S5000

Syntax

```
dot1x tx-period seconds
```

To return to the default, use the `no dot1x tx-period` command.

Parameters

seconds	Enter the interval time, in seconds, that EAPOL PDUs are transmitted. The range is 1 to 65535. The default is **30**.

Defaults	**30** seconds
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

show dot1x cos-mapping interface

Display the CoS priority-mapping table the RADIUS server provides and applied to authenticated supplicants on an 802.1X-enabled

S5000

Syntax

```
show dot1x cos-mapping interface type slot/port [mac-address
mac-address]
```

Parameters

interface ***type slot/port***	Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

mac-address	(Optional) MAC address of an 802.1X-authenticated supplicant.

Defaults

none

Command Modes

- EXEC
- EXEC privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Enter a supplicant's MAC address using the `mac-address` option to display CoS mapping information only for the specified supplicant.

You can display the CoS mapping information applied to traffic from authenticated supplicants on 802.1X-enabled ports that are in Single-Hot, Multi-Host, and Multi-Supplicant authentication modes.

Example

```
FTOS#show dot1x cos-mapping interface tengigabitethernet 2/21

802.1p CoS re-map table on Te 2/21:
----------------------------------
Dot1p   Remapped Dot1p
0       7
1       6
2       5
3       4
4       3
5       2
6       1
7       0

FTOS#show dot1x cos-mapping int te 2/21 mac-address
00:00:01:00:07:00

802.1p CoS re-map table on Te 2/21:
----------------------------------

802.1p CoS re-map table for Supplicant: 00:00:01:00:07:00
Dot1    Remapped Dot1p
0       7
1       6
2       5
3       4
4       3
5       2
6       1
7       0
```

show dot1x interface

Display the 802.1X configuration of an interface.

S5000

Syntax

`show dot1x interface type slot/port [mac-address mac-address]`

Parameters

interface *type slot/port*	Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
mac-address	(Optional) MAC address of a supplicant.

Defaults

none

Command Modes

- EXEC
- EXEC privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you enable 802.1X multi-supplicant authentication on a port, additional 802.1X configuration details (Port Authentication status, Untagged VLAN ID, Authentication PAE state, and Backend state) are displayed for each supplicant, as shown in the Example below.

Example (Interface)

```
FTOS#show dot1x int te 2/32

802.1x information on Te 2/32:
-----------------------------
Dot1x Status:            Enable
Port Control:            AUTO
Port Auth Status:        UNAUTHORIZED
Re-Authentication:       Disable
Untagged VLAN id:        None
Guest VLAN:              Enable
Guest VLAN id:           10
Auth-Fail VLAN:          Enable
Auth-Fail VLAN id:       11
Auth-Fail Max-Attempts: 3
Tx Period:               30 seconds
Quiet Period:            60 seconds
ReAuth Max:              2
Supplicant Timeout:      30 seconds
Server Timeout:          30 seconds
Re-Auth Interval:        3600 seconds
Max-EAP-Req:             2
Auth Type:               SINGLE_HOST
Auth PAE State:         Initialize
Backend State:          Initialize
FTOS#
```

Example (mac-address)

```
FTOS#show dot1x interface te 2/21 mac-address 00:00:01:00:07:00

802.1x information on Te 2/21:
-----------------------------
Dot1x Status:           Enable
Port Control:           AUTO
Re-Authentication:      Disable
Guest VLAN:             Disable
Guest VLAN id:          NONE
Auth-Fail VLAN:         Disable
Auth-Fail VLAN id:      NONE
Auth-Fail Max-Attempts: NONE
Mac-Auth-Bypass:        Enable
Mac-Auth-Bypass Only:   Disable
Tx Period:              5 seconds
Quiet Period:           60 seconds
ReAuth Max:             1
Supplicant Timeout:     30 seconds
Server Timeout:         30 seconds
Re-Auth Interval:       60 seconds
Max-EAP-Req:            2
Host Mode:              MULTI_AUTH
Max-Supplicants:        128

Port status and State info for Supplicant: 00:00:01:00:07:00

Port Auth Status:       AUTHORIZED(MAC-AUTH-BYPASS)
Untagged VLAN id:       4094
Auth PAE State:         Authenticated
Backend State:          Idle
FTOS#
```

7

Boot User Mode

All commands in this chapter are available in Boot User mode on the S5000.

To access this mode, press any key when the following line appears on the console during a system boot:

```
Hit any key to stop autoboot:
```

You enter Boot User mode immediately, as indicated by the `BOOT_USER#` prompt.

NOTE: You cannot use the Tab key to complete commands in this mode.

boot change

Change the boot parameters in the operating system.

S5000

Syntax

```
boot change {primary | secondary | default}
```

Command Modes BOOT USER

Parameters

primary	Set the S5000 to boot up with the primary boot parameters.
secondary	Set the S5000 to boot up with the secondary boot parameters.
default	Set the S5000 to boot up with the default boot parameters.

Default The S5000 boots up using the primary boot parameters if they are valid. If the primary parameters are not valid, the switch boots with the secondary parameters. If the secondary parameters are not valid, it boots with the default parameters.

Command History

Version 9.0(1.3)	Introduced on the S5000.

boot messages disable

Deactivate the NetBSD boot log. By default, the NetBSD log is disabled.

S5000

Syntax

```
boot messages disable
```

Command Modes	BOOT USER
Command History	**Version 9.0(1.3)** Introduced on the S5000.

boot messages enable

Enable the NetBSD boot log. By default, the NetBSD log is disabled.

S5000

Syntax	`boot messages enable`
Command Modes	BOOT USER
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Notes	Dell recommends that the NetBSD log remain disabled on the S5000. Use the `boot messages enable` command only if you need to debug S5000 operation.

boot show net config retries

Display the number of retries for a network boot configuration failure.

S5000

Syntax	`boot show net config retries`
Command Modes	BOOT USER
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
BOOT_USER# boot show net config retries
```

Number of Network Boot Config Retries is : 0

boot write net config retries

Set the number of retries used for a network boot configuration failure.

S5000

Syntax	`boot write net config retries` *`number`*
Command Modes	BOOT USER
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Example	`BOOT_USER# boot write net config retries 2` Updated number of Network Boot Config retries to 2.

boot zero

Clear the primary, secondary, or default boot parameters in the operating system.

S5000

Syntax	`boot zero {primary | secondary | default}`
Command Modes	BOOT USER
Command History	**Version 9.0(1.3)** Introduced on the S5000.

default gateway

Set the IP address of the default gateway.

S5000

Syntax	`default gateway` *`ip-address`*
Command Modes	BOOT USER
Command History	**Version 9.0(1.3)** Introduced on the S5000.

enable

Set the access privilege level.

S5000

Syntax	`enable {user | admin}`
Command Modes	BOOT USER
Command History	**Version 9.0(1.3)** Introduced on the S5000.

help

Display the Help menu.

S5000

Syntax	`help`
Command Modes	BOOT USER
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
BOOT_USER # help
***** Dell Force10 Boot Interface Help Information *****
Current access level: USER LEVEL
Use "syntax help" for more information on syntax.
Available command list (30 commands total):
  boot change [primary|secondary|default]
      change operating system boot parameters
  boot messages disable
      turn off netbsd boot messages
  boot messages enable
      turn on netbsd boot messages
  boot show net config retries
      show number of retries for network boot config failure
  boot write net config retries <int>
      write number of retries for network boot config failure
  boot zero [primary|secondary|default]
      zero operating system boot parameters
  default-gateway <ip-address>
default-gateway - set the default gateway ip address
  enable [user|admin]
      change access privilege level
-(26%)-Use <CR> to continue, q to stop:
  help
      display help menu
  ignore enable-password
      ignore enable password
  ignore startup-config
      ignore system starup-config
  interface management ethernet ip address <ip/mask>
```

```
set the management port ip address and mask
  interface management port config 1000m
      set the management port at 1000m
  interface management port config 100m
      set the management port at 100m
  interface management port config 10m
      set the management port at 10m
  interface management port config auto-negotiate
      set the management port to auto negotiate
  interface management port config full-duplex
      set the management port to full-duplex
  interface management port config half-duplex
      set the management port to half-duplex
-(60%)-Use <CR>> to continue, q to stop:
  interface management port config no auto-negotiate
      set the management port to no auto negotiate. set speed
and duplex to def
      ault values of (100m/full-duplex)
  no default-gateway
      clear the default gateway ip address
  no interface management ethernet ip address
      clear the management port ip address and mask
  reload
      reload entire chassis
  show boot blc
      show the boot loop counter value
  show boot selection
      display rom bootstrap bootflash partition
  show bootflash
      summary display of boot flash information
  show bootvar
      summary display of operating system boot parameters
  show default-gateway
      display the default gateway ip address
  show interface management ethernet
      display the management port ip address and mask
-(93%)-Use <CR>to continue, q to stop:
  show interface management port config
      show the management port boot characteristics
  syntax help
      show syntax information
```

ignore enable password

Ignore the enabled password.

S5000

Syntax	`ignore enable password`
Command Modes	BOOT USER
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ignore startup config

Ignore the system startup configuration.

S5000

Syntax

```
ignore startup config
```

Command Modes BOOT USER

Command History

Version 9.0(1.3)	Introduced on the S5000.

interface management ethernet ip address

Set the IP address and mask of the management port.

S5000

Syntax

```
interface management ethernet ip address ip-address/mask
```

Command Modes BOOT USER

Command History

Version 9.0(1.3)	Introduced on the S5000.

interface management port config

Set the speed or transmission mode of the management port.

S5000

Syntax

```
interface management port config {10m | 100m | 1000m | auto-
negotiate | no auto-negotiate | full-duplex | half-duplex}
```

Parameters

10m	Set the management port to operate at 10 Mbps.
100m	Set the management port to operate at 100 Mbps.
1000m	Set the management port to operate at 1000 Mbps.
auto-negotiate	Set the management port to auto-negotiate its speed with a peer device.
no auto-negotiate	Remove auto-negotiation from the management port and reset it to the default values (transmit at 100 Mbps in full-duplex mode).

full-duplex	Set the management port to transmit in full-duplex mode.
half-duplex	Set the management port to transmit in half-duplex mode.

Default	The management port transmits at 100 Mbps in full-duplex mode.
Command Modes	BOOT USER

Command History

Version 9.0(1.3)	Introduced on the S5000.

no default-gateway

Clear the IP address of the default gateway.

S5000

Syntax	`no default—gateway`
Command Modes	BOOT USER

Command History

Version 9.0(1.3)	Introduced on the S5000.

no interface management ethernet ip address

Clear the IP address and mask of the management port.

S5000

Syntax	`no interface management ethernet ip address`
Command Modes	BOOT USER

Command History

Version 9.0(1.3)	Introduced on the S5000.

reload

Reload the S5000 switch.

S5000

Syntax	`reload`
Command Modes	BOOT USER
Command History	**Version 9.0(1.3)** Introduced on the S5000.

show boot blc

Display the current boot-loop counter value.

S5000

Syntax	`show boot blc`
Command Modes	BOOT USER
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
BOOT_USER # show boot blc

Boot Loop Counter : 3
```

show boot selection

Display the currently selected bootflash partition to be used for a ROM bootstrap operation.

S5000

Syntax	`show boot selection`
Command Modes	BOOT USER
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
BOOT_USER # show boot selection

ROM BOOTSTRAP SELECTOR PARMETERS:
================================
Next ROM bootstrap set to occur from Bootflash partition A.
Last ROM bootstrap occurred from Bootflash partition B.
```

show bootflash

Display information about boot flash memory.

S5000

Syntax `show bootflash`

Command Modes BOOT USER

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
BOOT_USER # show bootflash

GENERAL BOOTFLASH INFO
======================
Bootflash Partition A:
  Dell Force10 Networks System Boot
  Official S5000_LP_IMG_BOOT_LOADER, BSP Release 1.3.1.2
  Created Thu May  9 12:01:34 2013 by build on tools-sjc-01

Bootflash Partition B:
  Dell Force10 Networks System Boot
  Official S5000_LP_IMG_BOOT_LOADER, BSP Release 1.3.1.2
  Created Thu May  9 19:24:22 2013 by build on tools-sjc-01

Boot Selector Partition:
  Dell Force10 Networks System Boot
  Official S5000_BTSEL_LP_IMG_BOOT_SELECTOR, BSP Release
1.3.0.1
  Created Thu May  9 19:24:23 2013 by build on tools-sjc-01

BOOT_USER #
```

show bootvar

Display information about the boot parameters used in the operating system.

S5000

Syntax `show bootvar`

Command Modes BOOT USER

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
BOOT_USER # show bootvar

PRIMARY OPERATING SYSTEM BOOT PARAMETERS:
========================================
boot device                        : flash
file name                          : systema (FTOS system://A
Partition)

SECONDARY OPERATING SYSTEM BOOT PARAMETERS:
========================================
boot device                        : flash
file name                          : systemb (FTOS system://B
Partition)

DEFAULT OPERATING SYSTEM BOOT PARAMETERS:
========================================
boot device                        : flash
file name                          : systema (FTOS system://A
Partition)

BOOT_USER #
```

show default-gateway

Display the IP address of the default gateway.

S5000

Syntax `show default-gateway`

Command Modes BOOT USER

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
BOOT_USER # show default-gateway

Gateway IP address: 10.11.210.63
```

show interface management ethernet

Display the IP address and mask of the management port.

S5000

Syntax `show interface management ethernet`

Command Modes BOOT USER

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
BOOT_USER # show interface management ethernet

Management ethernet IP address: 10.11.210.35/16
```

show interface management port config

Display configuration information about the management port.

S5000

Syntax `show interface management port config`

Command Modes BOOT USER

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
BOOT_USER # show inter management port conf

Management ethernet Port Configuration: Auto Negotiate
```

8

Access Control Lists (ACL)

Access control lists (ACLs) are supported on the S5000 switch.

FTOS supports the following types of ACL, IP prefix list, and route maps:

- Commands Common to all ACL Types
- Common IP ACL Commands
- Standard IP ACL Commands
- Extended IP ACL Commands
- Common MAC Access List Commands
- Standard MAC ACL Commands
- Extended MAC ACL Commands
- IP Prefix List Commands
- Route Map Commands
- AS-Path Commands
- IP Community List Commands

NOTE: For ACL commands that use the Trace function, refer to the Trace List Commands section in the Security chapter.

NOTE: For IPv6 ACL commands, refer to IPv6 Access Control Lists (IPv6 ACLs).

Commands Common to all ACL Types

The following commands are available within each ACL mode and do not have mode-specific options. Some commands in this chapter may use similar names, but require different options to support the different ACL types (for example, the `deny` and `permit` commands).

description

Configure a short text string describing the ACL.

S5000

Syntax	`description text`	
Parameters	*text*	Enter a text string up to 80 characters long.

Defaults

Not enabled.

Command Modes

- CONFIGURATION-STANDARD-ACCESS-LIST
- CONFIGURATION-EXTENDED-ACCESS-LIST
- CONFIGURATION-MAC ACCESS LIST-STANDARD
- CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

Version 9.0(1.3)	Introduced on the S5000.

remark

Enter a description for an ACL entry.

S5000

Syntax

`remark [remark-number] [description]`

Parameters

remark-number	Enter the remark number. The range is 0 to 4294967290. **NOTE:** You can use the same sequence number for the remark and an ACL rule.
description	Enter a description of up to 80 characters.

Defaults

Not configured.

Command Modes

- CONFIGURATION-STANDARD-ACCESS-LIST
- CONFIGURATION-EXTENDED-ACCESS-LIST
- CONFIGURATION-MAC ACCESS LIST-STANDARD
- CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `remark` command is available in each ACL mode. You can configure up to 4294967290 remarks in a given ACL.

The example below shows the use of the `remark` command twice within CONFIGURATION-STANDARD-ACCESS-LIST mode. The same sequence number was used for the remark and for an associated ACL rule. The remark precedes the rule in the running-config because it is assumed that the remark is for the rule with the same sequence number, or the group of rules that follow the remark.

Example

```
FTOS(config-std-nacl)#remark 10 Deny rest of the traffic
FTOS(config-std-nacl)#remark 5 Permit traffic from XYZ Inc.
FTOS(config-std-nacl)#show config
```

```
!
ip access-list standard test
remark 5 Permit traffic from XYZ Inc.
seq 5 permit 1.1.1.0/24
remark 10 Deny rest of the traffic
seq 10 Deny any
FTOS(config-std-nacl)#
```

Related Commands

show config – displays the current ACL configuration.

show config

Display the current ACL configuration.

S5000

Syntax

```
show config
```

Command Modes

- CONFIGURATION-STANDARD-ACCESS-LIST
- CONFIGURATION-EXTENDED-ACCESS-LIST
- CONFIGURATION-MAC ACCESS LIST-STANDARD
- CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(config-ext-nacl)#show conf
!
ip access-list extended patches
FTOS(config-ext-nacl)#
```

Common IP ACL Commands

The following commands are available within both IP ACL modes (Standard and Extended) and do not have mode-specific options. When an ACL is created without a rule and then is applied to an interface, ACL behavior reflects an implicit permit.

NOTE: Also refer to the Commands Common to all ACL Types section.

access-class

Apply a standard ACL to a terminal line.

S5000

Syntax

```
access-class access-list-name
```

Parameters

access-list-name	Enter the name of a configured Standard ACL, up to 140 characters.

Defaults Not configured.

Command Modes LINE

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear counters ip access-group

Erase all counters maintained for access lists.

S5000

Syntax

```
clear counters ip access-group [access-list-name]
```

Parameters

access-list-name	(OPTIONAL) Enter the name of a configured access-list, up to 140 characters.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip access-group

Assign an IP access list (IP ACL) to an interface.

S5000

Syntax

```
ip access-group access-list-name {in} [implicit-permit] [vlan
vlan-id]
```

Parameters

access-list-name	Enter the name of a configured access list, up to 140 characters.

in	Enter the keyword `in` to apply the ACL to incoming traffic.
implicit-permit	(OPTIONAL) Enter the keyword `implicit-permit` to change the default action of the ACL from implicit-deny to implicit-permit (that is, if the traffic does not match the filters in the ACL, the traffic is permitted instead of dropped).
vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` followed by the ID numbers of the VLANs.

Defaults

Not enabled.

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can assign one ACL (standard or extended ACL) to an interface.

NOTE: This command does not support S5000 Loopback interfaces.

When you apply an ACL that filters IGMP traffic, all IGMP traffic is redirected to the CPUs and soft-forwarded, if required, in the following scenarios:

- on a Layer 2 interface - if a Layer 3 ACL is applied to the interface
- on a Layer 3 port or on a Layer 2/Layer 3 port

Related Commands

ip access-list standard – configures a standard ACL.

ip access-list extended – configures an extended ACL.

show ip access-lists

Display all of the IP ACLs configured in the system, whether or not they are applied to an interface, and the count of matches/mismatches against each ACL entry displayed.

S5000

Syntax

```
show ip access-lists [access-list-name] [interface type slot/
port] [in | out]
```

Parameters

access-list-name	Enter the name of a configured MAC ACL, up to 140 characters.
interface *type slot/port*	Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

in | out	Identify whether ACL is applied on the ingress or egress side.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip accounting access-list

Display the IP access-lists created on the switch and the sequence of filters.

S5000

Syntax

```
show ip accounting {access-list list-name | cam_count}
interface type slot/port
```

Parameters

access-list-name	Enter the name of the ACL to be displayed.
cam_count	List the count of the CAM rules for this ACL.
interface *type slot/port*	Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
in | out	Identify whether ACL is applied on the ingress or egress side.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Field	Description
"Extended IP..."	Displays the name of the IP ACL.
"seq 5..."	Displays the filter. If the keywords `count` or `byte` were configured in the filter, the number of packets or bytes processed by the filter is displayed at the end of the line.
"order 4"	Displays the QoS order of priority for the ACL entry.

Example

```
FTOS#show ip accounting access FILTER1 interface te 1/6
Extended IP access list FILTER1
seq 5 deny ip any 191.1.0.0 /16 count (0x00 packets)
seq 10 deny ip any 191.2.0.0 /16 order 4
seq 15 deny ip any 191.3.0.0 /16
seq 20 deny ip any 191.4.0.0 /16
seq 25 deny ip any 191.5.0.0 /16
```

Standard IP ACL Commands

When you create an ACL without any rule and then apply it to an interface, the ACL behavior reflects an implicit permit.

NOTE: Also refer to the Commands Common to all ACL Types and Common IP ACL Commands sections.

deny

Configure a filter to drop packets with a certain IP address.

S5000

Syntax

```
deny {source [mask] | any | host ip-address} [count [byte] |
log] [dscp value] [order] [monitor] [fragments]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {source [mask] | any | host ip-address}` command.

Parameters

source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous (discontiguous).

any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address only.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS order of priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority). The default is, if you do not use the keyword `order`, the ACLs have the lowest order by default (255).
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. **NOTE:** For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *FTOS Configuration Guide*.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.

Defaults Not configured.

Command Modes CONFIGURATION-STANDARD-ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *FTOS Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to the Port Monitoring chapter.

The S5000 cannot count both packets and bytes, when you enter the count byte options, only bytes are incremented.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

ip access-list standard – configures a standard ACL.

permit – configures a permit filter.

ip access-list standard

Create a standard IP access list (IP ACL) to filter based on IP address.

S5000

Syntax `ip access-list standard access-list-name`

Parameters

access-list-name	Enter a string up to 140 characters long as the ACL name.

Defaults All IP access lists contain an implicit "deny any," that is, if no match occurs, the packet is dropped.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

FTOS supports one ingress and one egress IP ACL per interface.

The number of entries allowed per ACL is hardware-dependent. For detailed specifications on entries allowed per ACL, refer to your switch documentation.

Example

```
FTOS(conf)#ip access-list standard TestList
FTOS(config-std-nacl)#
```

Related Commands

ip access-list extended – creates an extended access list.

show config – displays the current configuration.

permit

Configure a filter to permit packets from a specific source IP address to leave the switch.

S5000

Syntax

```
permit {source [mask] | any | host ip-address} [count [byte]]
[dscp value] [order] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit {source [mask] | any | host ip-address}` command.

Parameters

source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address or hostname.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. **NOTE:** For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the *FTOS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-STANDARD-ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the “Quality of Service” chapter of the *FTOS Configuration Guide*.

When you use the `log` option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to Port Monitoring

TheS5000 cannot count both packets and bytes; when you enter the count byte options, only bytes are incremented.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny – Assigns a IP ACL filter to deny IP packets.

ip access-list standard – creates a standard ACL.

resequence access-list

Re-assign sequence numbers to entries of an existing access-list.

S5000

Syntax

resequence access-list {ipv4 | ipv6 | mac} {*access-list-name StartingSeqNum Step-to-Increment*}

Parameters

ipv4 | ipv6 | mac	Enter the keyword `ipv4`or `mac` to identify the access list type to resequence.
access-list-name	Enter the name of a configured IP access list.
StartingSeqNum	Enter the starting sequence number to resequence. The range is 0 to 4294967290.
Step-to-Increment	Enter the step to increment the sequence number. The range is 1 to 4294967290.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you have exhausted all the sequence numbers, this feature permits re-assigning a new sequence number to entries of an existing access-list.

Related Commands

resequence prefix-list ipv4 – resequences a prefix list.

resequence prefix-list ipv4

Re-assign sequence numbers to entries of an existing prefix list.

S5000

Syntax

```
resequence prefix-list ipv4 {prefix-list-name StartingSeqNum
Step-to-increment}
```

Parameters

prefix-list-name	Enter the name of the configured prefix list, up to 140 characters long.
StartingSeqNum	Enter the starting sequence number to resequence. The range is 0 to 65535.
Step-to-Increment	Enter the step to increment the sequence number. The range is 1 to 65535.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you have exhausted all the sequence numbers, this feature permits re-assigning a new sequence number to entries of an existing prefix list.

Related Commands

resequence access-list – resequences an access-list.

seq

Assign a sequence number to a deny or permit filter in an IP access list while creating the filter.

S5000

Syntax

seq *sequence-number* {deny | permit} {*source* [*mask*] | any | host *ip-address*}} [count [byte]] [dscp *value*] [order] [monitor] [fragments]

Parameters

sequence-number	Enter a number from 0 to 4294967290.The range is 0 to 65534.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.

source	Enter a IP address in dotted decimal format of the network from which the packet was received.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address or hostname.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS order for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. **NOTE:** For more information, refer to the Flow-based Monitoring section in the Port Monitoring chapter of the *FTOS Configuration Guide*.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.

Defaults Not configured

Command Modes CONFIGURATION-STANDARD-ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to Port Monitoring.

The `order` option is relevant in the context of the Policy QoS feature only. The following applies:

- The `seq` *`sequence-number`* command is applicable only in an ACL group.
- The `order` option works across ACL groups that have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq` *`sequence-number`*.

- If *sequence-number* is not configured, the rules with the same order value are ordered according to their configuration order.
- If *sequence-number* is configured, the sequence-number is used as a tie breaker for rules with the same order.

When you use the `log` option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny – configures a filter to drop packets.

permit – configures a filter to forward packets.

Extended IP ACL Commands

When an ACL is created without any rule and then applied to an interface, ACL behavior reflects an implicit permit.

The following commands configure extended IP ACLs, which in addition to the IP address, also examine the packet's protocol type.

NOTE: Also refer to the Commands Common to all ACL Types and Common IP ACL Commands sections.

deny

Configure a filter that drops IP packets meeting the filter criteria.

S5000

Syntax

```
deny {ip | ip-protocol-number} {source mask | any | host ip-address} {destination mask | any | host ip-address} [count [byte]] [dscp value] [order] [monitor] [fragments]
```

To remove this filter, you have two choices:

- Use the `no seq` *sequence-number* command if you know the filter's sequence number.
- Use the `no deny {ip |` *ip-protocol-number*`} {`*source mask*` | any | host `*ip-address*`} {`*destination mask*` | any | host `*ip-address*`}` command.

Parameters

ip	Enter the keyword `ip` to configure a generic IP access list. The keyword `ip` specifies that the access list denies all IP protocols.
ip-protocol-number	Enter a number from 0 to 255 to deny based on the protocol identified in the IP protocol header.

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or noncontiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword `count` to count packets that the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes that the filter processes.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *FTOS Configuration Guide*.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *FTOS Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to the Port Monitoring chapter.

The S5000 cannot count both packets and bytes, when you enter the count byte options, only bytes are incremented.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny tcp – assigns a filter to deny TCP packets.

deny udp – assigns a filter to deny UDP packets.

ip access-list extended – creates an extended ACL.

deny tcp

Configure a filter that drops transmission control protocol (TCP) packets meeting the filter criteria.

S5000

Syntax

```
deny tcp {source mask | any | host ip-address} [bit] [operator
port [port]] {destination mask | any | host ip-address} [dscp]
[bit] [operator port [port]] [count [byte]] [order] [monitor]
[fragments]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny tcp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address.
dscp	Enter this keyword `dscp` to deny a packet based on the DSCP value. The range is 0 to 63.
bit	Enter a flag or combination of bits: • `ack`: acknowledgement field • `fin`: finish (no more data from the user) • `psh`: push function • `rst`: reset the connection • `syn`: synchronize sequence numbers • `urg`: urgent field

operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the `port` command)
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) If you did not use the keyword `order`, the ACLs have the lowest order by default (255).
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *FTOS Configuration Guide*.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *FTOS Configuration Guide*.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to the Port Monitoring chapter.

When you use the `log` option, the CP processor logs details the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

The S5000 cannot count both packets and bytes; when you enter the count byte options, only bytes are incremented.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt, or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Rule#  Data              Mask         From To #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Rule# Data              Mask         From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024

Total Ports: 1024
```

Related Commands

deny – assigns a filter to deny IP traffic.

deny udp – assigns a filter to deny UDP traffic.

deny udp

Configure a filter to drop user datagram protocol (UDP) packets meeting the filter criteria.

S5000

Syntax

```
deny udp {source mask | any | host ip-address} [operator port
[port]] {destination mask | any | host ip-address} [dscp]
```

```
[operator port [port]] [count [byte]] [order] [monitor]
[fragments]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no deny udp {`*`source mask`*` | any | host `*`ip-address`*`} {`*`destination mask`*` | any | host `*`ip-address`*`}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address.
dscp	Enter this keyword `dscp` to deny a packet based on the DSCP value. The range is 0 to 63.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the `port` command)
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is 0 to 65535.
destination	Enter the IP address of the network or host to which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) If you did not use the keyword `order`, the ACLs have the lowest order by default (255).

monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the section “Flow-based Monitoring” in the Port Monitoring chapter of the *FTOS Configuration Guide*.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *FTOS Configuration Guide*.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to the Port Monitoring chapter.

When you use the `log` option, the CP processor logs details the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

The S5000 cannot count both packets and bytes; when you enter the count byte options, only bytes are incremented.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Rule#  Data             Mask        From To #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Rule# Data              Mask        From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024

Total Ports: 1024
```

Related Commands	deny – assigns a filter to deny IP traffic. deny tcp – assigns a filter to deny TCP traffic.

ip access-list extended

Name (or select) an extended IP access list (IP ACL) based on IP addresses or protocols.

S5000

Syntax

`ip access-list extended` *`access-list-name`*

To delete an access list, use the `no ip access-list extended` *`access-list-name`* command.

Parameters

access-list-name	Enter a string up to 140 characters long as the access list name.

Defaults

All access lists contain an implicit “deny any”; that is, if no match occurs, the packet is dropped.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The number of entries allowed per ACL is hardware-dependent. For detailed specification on entries allowed per ACL, refer to your switch documentation.

Example

```
FTOS(conf)#ip access-list extended TESTListEXTEND
FTOS(config-ext-nacl)#
```

Related Commands

ip access-list standard – configures a standard IP access list.

show config – displays the current configuration.

permit

Configure a filter to pass IP packets meeting the filter criteria.

S5000

Syntax

`permit {ip |` *`ip-protocol-number`*`} {`*`source mask`* `| any | host` *`ip-address`*`} {`*`destination mask`* `| any | host` *`ip-address`*`} [count [byte]] [dscp` *`value`*`] [order] [monitor] [fragments]`

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter’s sequence number.

- Use the `no deny {ip | ip-protocol-number} {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

ip	Enter the keyword `ip` to configure a generic IP access list. The keyword `ip` specifies that the access list will permit all IP protocols.
ip-protocol-number	Enter a number from 0 to 255 to permit based on the protocol identified in the IP protocol header. The range is 0 to 128.
source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address or hostname.
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. **NOTE:** For more information, refer to the Flow-based Monitoring section in the Port Monitoring chapter of the *FTOS Configuration Guide*.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the “Quality of Service” chapter of the *FTOS Configuration Guide*.

When you use the `log` option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to Port Monitoring.

The S5000 cannot count both packets and bytes; when you enter the count byte options, only bytes are incremented.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

ip access-list extended – creates an extended ACL.

permit tcp – assigns a permit filter for TCP packets.

permit udp – assigns a permit filter for UDP packets.

permit tcp

Configure a filter to pass TCP packets meeting the filter criteria.

S5000

Syntax

```
permit tcp {source mask | any | host ip-address} [bit]
[operator port [port]] {destination mask | any | host ip-
address} [bit] [dscp] [operator port [port]] [count [byte]]
[order] [monitor] [fragments]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter’s sequence number.
- Use the `no permit tcp {`*`source mask`*` | any | host `*`ip-address`*`} {`*`destination mask`*` | any | host `*`ip-address`*`}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.

host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address.
bit	Enter a flag or combination of bits: • `ack:` acknowledgement field • `fin:` finish (no more data from the user) • `psh:` push function • `rst:` reset the connection • `syn:` synchronize sequence numbers • `urg:` urgent field
dscp	Enter the keyword `dscp` to deny a packet based on the DSCP value. The range is 0 to 63.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the port parameter)
port port	Enter the application layer port number. Enter two port numbers if you are using the range logical operand. The range is 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).

monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. **NOTE:** For more information, refer to the Flow-based Monitoring section in the Port Monitoring chapter of the *FTOS Configuration Guide*.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.

Defaults

Not configured.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the “Quality of Service” chapter of the *FTOS Configuration Guide*.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

When you use the `log` option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

The S5000 cannot count both packets and bytes; when you enter the count byte options, only bytes are incremented.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to Port Monitoring.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt, or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Rule# Data                Mask             From To   #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Rule# Data               Mask              From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024
```

```
Total Ports: 1024
```

Related Commands

ip access-list extended – creates an extended ACL.

permit – assigns a permit filter for IP packets.

permit udp – assigns a permit filter for UDP packets.

permit udp

Configure a filter to pass UDP packets meeting the filter criteria.

S5000

Syntax

```
permit udp {source mask | any | host ip-address} [operator port
[port]] {destination mask | any | host ip-address} [dscp]
[operator port [port]] [count [byte]] [order] [monitor]
[fragments]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no permit udp {`*`source mask`*` | any | host `*`ip-address`*`} {`*`destination mask`*` | any | host `*`ip-address`* command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address.
dscp	Enter the keyword `dscp` to deny a packet based on the DSCP value. The range is 0 to 63.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the `port` parameter)

port port	Enter the application layer port number. Enter two port numbers if you are using the `range` logical operand. The range is 0 to 65535.
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. **NOTE:** For more information, refer to the Flow-based Monitoring section in the Port Monitoring chapter of the *FTOS Configuration Guide*.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the “Quality of Service” chapter of the *FTOS Configuration Guide*.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

When you use the `log` option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

The S5000 cannot count both packets and bytes; when you enter the count byte options, only bytes are incremented.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to Port Monitoring.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt, or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Rule# Data             Mask         From To   #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Rule# Data            Mask          From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024

Total Ports: 1024
```

Related Commands

ip access-list extended – creates an extended ACL.

permit – assigns a permit filter for IP packets.

permit tcp – assigns a permit filter for TCP packets.

resequence access-list

Re-assign sequence numbers to entries of an existing access-list.

S5000

Syntax

`resequence access-list {ipv4 | mac} {`*`access-list-name StartingSeqNum Step-to-Increment`*`}`

Parameters

ipv4 | mac	Enter the keyword `ipv4`or `mac` to identify the access list type to resequence.
access-list-name	Enter the name of a configured IP access list, up to 140 characters.
StartingSeqNum	Enter the starting sequence number to resequence. The range is 0 to 4294967290.
Step-to-Increment	Enter the step to increment the sequence number. The range is 1 to 4294967290.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When all sequence numbers have been exhausted, this feature permits re-assigning a new sequence number to entries of an existing access-list.

Related Commands

resequence prefix-list ipv4 – resequences a prefix list.

resequence prefix-list ipv4

Re-assign sequence numbers to entries of an existing prefix list.

S5000

Syntax

```
resequence prefix-list ipv4 {prefix-list-name StartingSeqNum
Step-to-increment}
```

Parameters

prefix-list-name	Enter the name of the configured prefix list, up to 140 characters long.
StartingSeqNum	Enter the starting sequence number to resequence. The range is 0 to 65535.
Step-to-Increment	Enter the step to increment the sequence number. The range is 1 to 65535.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you have exhausted all the sequence numbers, this feature permits re-assigning a new sequence number to entries of an existing prefix list.

Related Commands

resequence access-list – resequences an access-list.

seq

Assign a sequence number to a deny or permit filter in an extended IP access list while creating the filter.

S5000

Syntax

```
seq sequence-number {deny | permit} {ip-protocol-number | icmp
| ip | tcp | udp} {source mask | any | host ip-address}
{destination mask | any | host ip-address} [operator port
[port]] [count [byte]] [dscp value] [order] [monitor]
[fragments]
```

Parameters

sequence-number	Enter a number from 0 to 4294967290. For the S4810, the range is 0 to 65534.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
ip-protocol-number	Enter a number from 0 to 255 to filter based on the protocol identified in the IP protocol header.
icmp	Enter the keyword `icmp` to configure an ICMP access list filter.
ip	Enter the keyword `ip` to configure a generic IP access list. The keyword `ip` specifies that the access list permits all IP protocols.
tcp	Enter the keyword `tcp` to configure a TCP access list filter.
udp	Enter the keyword `udp` to configure a UDP access list filter.
source	Enter a IP address in dotted decimal format of the network from which the packet was received.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address or hostname.
operator	(OPTIONAL) Enter one of the following logical operands: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the `port` parameter.)

port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if you are using the range logical operand. The range is 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
message-type	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type. The range is 0 to 255 for ICMP type and 0 to 255 for ICMP code.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DCSCP values.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS order for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. **NOTE:** For more information, refer to the Flow-based Monitoring section in the Port Monitoring chapter of the *FTOS Configuration Guide*.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.

Defaults Not configured

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to Port Monitoring.

The `order` option is relevant in the context of the Policy QoS feature only. The following applies:

- The `seq` *`sequence-number`* command is applicable only in an ACL group.
- The `order` option works across ACL groups that have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq` *`sequence-number`*.
- If *`sequence-number`* is not configured, the rules with the same order value are ordered according to their configuration order.
- If *`sequence-number`* is configured, the sequence-number is used as a tie breaker for rules with the same order.

When you use the `log` option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

If you configure the *`sequence-number`*, the *`sequence-number`* is used as a tie breaker for rules with the same order.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny – configures a filter to drop packets.

permit – configures a filter to forward packets.

Common MAC Access List Commands

The following commands are available within both MAC ACL modes (Standard and Extended) and do not have mode-specific options. These commands allow you to clear, display, and assign MAC ACL configurations.

clear counters mac access-group

Clear counters for all or a specific MAC ACL.

S5000

Syntax

```
clear counters mac access-group [mac-list-name]
```

Parameters

mac-list-name	(OPTIONAL) Enter the name of a configured MAC access list.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

mac access-group

Apply a MAC ACL to traffic entering or exiting an interface.

S5000

Syntax

```
mac access-group access-list-name {in [vlan vlan-range]}
```

Parameters

access-list-name	Enter the name of a configured MAC access list, up to 140 characters.
vlan *vlan-range*	(OPTIONAL) Enter the keyword `vlan` and then enter a range of VLANs. The range is 1 to 4094. **NOTE:** This option is available only with the keyword`in` option.
in	Enter the keyword `in` to configure the ACL to filter incoming traffic.

Defaults

none

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can assign one ACL (standard or extended) to an interface.

Related Commands

mac access-list standard – configures a standard MAC ACL.

mac access-list extended – configures an extended MAC ACL.

show mac access-lists

Display all of the Layer 2 ACLs configured in the system, whether or not they are applied to an interface, and the count of matches/mismatches against each ACL entry displayed.

S5000

Syntax

```
show mac access-lists [access-list-name] [interface type slot/
port] [in | out]
```

Parameters

list-name	Enter the name of a configured MAC ACL, up to 140 characters.
interface *type slot/port*	Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

in | out	Identify whether ACL is applied on ingress or egress side.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show mac accounting access-list

Display MAC access list configurations and counters (if configured).

S5000

Syntax

```
show mac accounting access-list access-list-name interface type
slot/port in | out
```

Parameters

access-list-name	Enter the name of a configured MAC ACL, up to 140 characters.
interface *type slot/port*	Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below.

- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

in | out	Identify whether an ACL is applied on the ingress or egress side.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The ACL hit counters in this command increment the counters for each matching rule, not just the first matching rule.

Example

```
FTOS#show mac accounting access-list mac-ext interface po 1
Extended mac access-list mac-ext on TenGigabitEthernet 0/11
  seq 5 permit host 00:00:00:00:00:11 host 00:00:00:00:00:19
count (393794576 packets)
  seq 10 deny  host 00:00:00:00:00:21 host 00:00:00:00:00:29
count (89076777 packets)
  seq 15 deny  host 00:00:00:00:00:31 host 00:00:00:00:00:39
count (0 packets)
  seq 20 deny  host 00:00:00:00:00:41 host 00:00:00:00:00:49
count (0 packets)
  seq 25 permit any any count (0 packets)
Extended mac access-list mac-ext on TenGigabitEthernet 0/12
  seq 5 permit host 00:00:00:00:00:11 host 00:00:00:00:00:19
count (57589834 packets)
  seq 10 deny  host 00:00:00:00:00:21 host 00:00:00:00:00:29
count (393143077 packets)
  seq 15 deny  host 00:00:00:00:00:31 host 00:00:00:00:00:39
count (0 packets)
  seq 20 deny  host 00:00:00:00:00:41 host 00:00:00:00:00:49
count (0 packets)
  seq 25 permit any any count (0 packets)
FTOS#
```

Standard MAC ACL Commands

When you create an access control list without any rule and then apply it to an interface, the ACL behavior reflects implicit permit. These commands configure standard MAC ACLs.

NOTE: For more information, also refer to the Commands Common to all ACL Types and Common MAC Access List Commands sections.

deny

Configure a filter to drop packets with a the MAC address specified.

S5000

Syntax

`deny {any | mac-source-address [mac-source-address-mask]} [count [byte]]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {any | mac-source-address mac-source-address-mask}` command.

Parameters

any	Enter the keyword `any` to specify that all routes are subject to the filter.

mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *FTOS Configuration Guide*.

Defaults Not enabled.

Command Modes CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

permit – configures a MAC address filter to pass packets.

seq – configures a MAC address filter with a specified sequence number.

mac access-list standard

Name a new or existing MAC access control list (MAC ACL) and enter MAC ACCESS LIST mode to configure a standard MAC ACL. Also refer to the Commands Common to all ACL Types section and the Common MAC Access List Commands section.

S5000

Syntax `mac access-list standard mac-list-name`

Parameters

mac-list-name	Enter a text string as the name of the standard MAC access list (140 character maximum).

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

FTOS supports one ingress and one egress MAC ACL per interface.

The number of entries allowed per ACL is hardware-dependent. For detailed specifications on entries allowed per ACL, refer to your switch documentation.

Example

```
FTOS(conf)#mac-access-list access-list standard TestMAC
FTOS(config-std-macl)#?
deny              Specify packets to reject
description       List description
exit              Exit from access-list configuration mode
no                Negate a command or set its defaults
permit            Specify packets to forward
remark            Specify access-list entry remark
seq               Sequence numbers
show              Show Standard ACL configuration
```

permit

Configure a filter to forward packets from a specific source MAC address.

S5000

Syntax

`permit {any | mac-source-address [mac-source-address-mask]} [count [byte]]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit {any | mac-source-address mac-source-address-mask}` command.

Parameters

any	Enter the keyword `any` to forward all packets received with a MAC address.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.

byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. **NOTE:** For more information, refer to the Flow-based Monitoring section in the Port Monitoring chapter of the *FTOS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you use the `log` option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny – configures a MAC ACL filter to drop packets.

seq – configure a MAC ACL filter with a specified sequence number.

seq

Assign a sequence number to a deny or permit filter in a MAC access list while creating the filter.

S5000

Syntax

```
seq sequence-number {deny | permit} {any | mac-source-address
[mac-source-address-mask]} [count [byte]] [monitor]
```

Parameters

sequence-number	Enter a number between 0 to 65535.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
any	Enter the keyword `any` to filter all packets.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.

mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. **NOTE:** For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the *FTOS Configuration Guide*.

Defaults

Not configured

Command Modes

CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you use the `log` option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny – configures a filter to drop packets.

permit – configures a filter to forward packets.

Extended MAC ACL Commands

When an access-list is created without any rule and then applied to an interface, ACL behavior reflects implicit permit. The following commands configure Extended MAC ACLs.

The S5000 switch supports Ingress MAC ACLs only.

NOTE: For more information, also refer to the Commands Common to all ACL Types and Common MAC Access List Commands sections.

deny

Configure a filter to drop packets that match the filter criteria.

S5000

Syntax

```
deny {any | host mac-address | mac-source-address mac-source-
address-mask} {any | host mac-address | mac-destination-address
mac-destination-address-mask} [ethertype-operator] [count
[byte]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no deny {any | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask}` command.

Parameters

any	Enter the keyword `any` to drop all packets.
host *mac-address*	Enter the keyword `host` and then enter a MAC address to drop packets with that host address.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
mac-destination-address	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
mac-destination-address-mask	Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
ethertype operator	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: • `ev2` - is the Ethernet II frame format • `llc` - is the IEEE 802.3 frame format • `snap` - is the IEEE 802.3 SNAP frame format
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.

monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the *FTOS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

permit – configures a MAC address filter to pass packets.

seq – configures a MAC address filter with a specified sequence number.

mac access-list extended

Name a new or existing extended MAC access control list (extended MAC ACL).

S5000

Syntax `mac access-list extended` *`access-list-name`*

Parameters

mac-list-name	Enter a text string as the MAC access list name, up to 140 characters.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The number of entries allowed per ACL is hardware-dependent. For detailed specifications on entries allowed per ACL, refer to your switch documentation.

Example

```
FTOS(conf)#mac-access-list access-list extended TestMATExt
FTOS(config-ext-macl)#remark 5 IPv4
FTOS(config-ext-macl)#seq 10 permit any any ev2 eq 800 count
bytes
FTOS(config-ext-macl)#remark 15 ARP
FTOS(config-ext-macl)#seq 20 permit any any ev2 eq 806 count
bytes
FTOS(config-ext-macl)#remark 25 IPv6
FTOS(config-ext-macl)#seq 30 permit any any ev2 eq 86dd count
bytes
FTOS(config-ext-macl)#seq 40 permit any any count bytes
FTOS(config-ext-macl)#exit
FTOS(conf)#do show mac accounting access-list snickers
interface g0/47 in
Extended mac access-list snickers on TenGigabitEthernet 0/47
seq 10 permit any any ev2 eq 800 count bytes (559851886
packets 191402152148
bytes)
seq 20 permit any any ev2 eq 806 count bytes (74481486 packets
5031686754
bytes)
seq 30 permit any any ev2 eq 86dd count bytes (7751519 packets
797843521 bytes)
```

Related Commands

mac access-list standard – configures a standard MAC access list.

show mac accounting access-list – displays MAC access list configurations and counters (if configured).

permit

Configure a filter to pass packets matching the criteria specified.

S5000

Syntax

`permit {any | host` *`mac-address`* `|` *`mac-source-address mac-source-address-mask`*`} {any | host` *`mac-address`* `|` *`mac-destination-address mac-destination-address-mask`*`} [`*`ethertype operator`*`] [count [byte]] | [monitor]`

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no permit {any | host` *`mac-address`* `|` *`mac-source-address mac-source-address-mask`*`} {any |` *`mac-destination-address mac-destination-address-mask`*`}` command.

Parameters

any	Enter the keyword `any` to forward all packets.
host	Enter the keyword `host` and then enter a MAC address to forward packets with that host address.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.

mac-destination-address	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
mac-destination-address-mask	Specify which bits in the MAC address must be matched. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
ethertype operator	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: • `ev2` - is the Ethernet II frame format • `llc` - is the IEEE 802.3 frame format • `snap` - is the IEEE 802.3 SNAP frame format
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. **NOTE:** For more information, refer to the Flow-based Monitoring section in the Port Monitoring chapter of the *FTOS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you use the `log` option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny – configures a MAC ACL filter to drop packets.

seq – configure a MAC ACL filter with a specified sequence number.

seq

Configure a filter with a specific sequence number.

S5000

Syntax

`seq sequence-number {deny | permit} {any | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask} [ethertype operator] [count [byte]] [monitor]`

Parameters

sequence-number	Enter a number as the filter sequence number. The range is zero (0) to 65535.
deny	Enter the keyword `deny` to drop any traffic matching this filter.
permit	Enter the keyword `permit` to forward any traffic matching this filter.
any	Enter the keyword `any` to filter all packets.
host *mac-address*	Enter the keyword `host` and then enter a MAC address to filter packets with that host address.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
mac-source-address-mask	Specify which bits in the MAC address must be matched.
mac-destination-address	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
mac-destination-address-mask	Specify which bits in the MAC address must be matched. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
ethertype operator	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: • `ev2` - is the Ethernet II frame format. • `llc` - is the IEEE 802.3 frame format. • `snap` - is the IEEE 802.3 SNAP frame format.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

NOTE: For more information, refer to the Flow-based Monitoring section in the Port Monitoring chapter of the *FTOS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information When you use the `log` option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny – configures a filter to drop packets.

permit – configures a filter to forward packets.

IP Prefix List Commands

When you create an access-list without any rule and then apply it to an interface, the ACL behavior reflects implicit permit.

Use these commands to configure or enable IP prefix lists.

clear ip prefix-list

Reset the number of times traffic mets the conditions ("hit" counters) of the configured prefix lists.

S5000

Syntax `clear ip prefix-list [prefix-name]`

Parameters

prefix-name	(OPTIONAL) Enter the name of the configured prefix list to clear only counters for that prefix list, up to 140 characters long.

Defaults Clears "hit" counters for all prefix lists unless a prefix list is specified.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands	ip prefix-list — configures a prefix list.

deny

Configure a filter to drop packets meeting the criteria specified.

S5000

Syntax

`deny ip-prefix [ge min-prefix-length] [le max-prefix-length]`

Parameters

ip-prefix	Specify an IP prefix in the network/length format. For example, 35.0.0.0/ 8 means match the first 8 bits of address 35.0.0.0.
ge *min-prefix-length*	(OPTIONAL) Enter the keyword `ge` and then enter the minimum prefix length, which is a number from zero (0) to 32.
le *max-prefix-length*	(OPTIONAL) Enter the keyword `le` and then enter the maximum prefix length, which is a number from zero (0) to 32.

Defaults	Not configured.
Command Modes	PREFIX-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Sequence numbers for this filter are automatically assigned starting at sequence number 5.

If you do not use the `ge` or `le` options, only packets with an exact match to the prefix are filtered.

Related Commands

permit – configures a filter to pass packets.

seq – configures a drop or permit filter with a specified sequence number.

ip prefix-list

Enter the PREFIX-LIST mode and configure a prefix list.

S5000

Syntax

`ip prefix-list prefix-name`

Parameters

prefix-name	Enter a string up to 16 characters long as the name of the prefix list, up to 140 characters long.

Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Prefix lists redistribute OSPF and RIP routes meeting specific criteria.
Related Commands	show ip route list – displays IP routes in an IP prefix list. show ip prefix-list summary – displays a summary of the configured prefix lists.

permit

Configure a filter that passes packets meeting the criteria specified.

S5000

Syntax

`permit ip-prefix [ge min-prefix-length] [le max-prefix-length]`

Parameters

ip-prefix	Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.
ge *min-prefix-length*	(OPTIONAL) Enter the keyword `ge` and then enter the minimum prefix length, which is a number from zero (0) to 32.
le *max-prefix-length*	(OPTIONAL) Enter the keyword `le` and then enter the maximum prefix length, which is a number from zero (0) to 32.

Command Modes	PREFIX-LIST
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Sequence numbers for this filter are automatically assigned starting at sequence number 5. If you do not use the `ge` or `le` options, only packets with an exact match to the prefix are filtered.
Related Commands	deny – configures a filter to drop packets. seq – configures a drop or permit filter with a specified sequence number.

seq

Assign a sequence number to a deny or permit filter in a prefix list while configuring the filter.

S5000

Syntax

```
seq sequence-number {deny | permit} {any} | [ip-prefix /nn {ge
min-prefix-length} {le max-prefix-length}] | [bitmask number]
```

Parameters

sequence-number	Enter a number. The range is 1 to 4294967294.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition..
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this condition.
any	(OPTIONAL) Enter the keyword `any` to match any packets.
ip-prefix /nn	(OPTIONAL) Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.
ge *min-prefix-length*	(OPTIONAL) Enter the keyword `ge` and then enter the minimum prefix length, which is a number from zero (0) to 32.
le *max-prefix-length*	(OPTIONAL) Enter the keyword `le` and then enter the maximum prefix length, which is a number from zero (0) to 32.
bitmask *number*	Enter the keyword `bitmask` and then enter a bit mask number in dotted decimal format.

Defaults Not configured.

Command Modes PREFIX-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you do not use the `ge` or `le` options, only packets with an exact match to the prefix are filtered.

Related Commands

deny – configures a filter to drop packets.

permit – configures a filter to pass packets.

show config

Display the current PREFIX-LIST configurations.

S5000

Syntax `show config`

Command Modes PREFIX-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-nprefixl)#show config
!
ip prefix-list snickers
FTOS(conf-nprefixl)#
```

show ip prefix-list detail

Display details of the configured prefix lists.

S5000

Syntax `show ip prefix-list detail [`*`prefix-name`*`]`

Parameters

prefix-name	(OPTIONAL) Enter a text string as the name of the prefix list, up to 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip prefix-list detail
Prefix-list with the last deletion/insertion: filter_ospf
ip prefix-list filter_in:
count: 3, range entries: 3, sequences: 5 - 10
  seq 5 deny 1.102.0.0/16 le 32 (hit count: 0)
  seq 6 deny 2.1.0.0/16 ge 23 (hit count: 0)
  seq 10 permit 0.0.0.0/0 le 32 (hit count: 0)
ip prefix-list filter_ospf:
count: 4, range entries: 1, sequences: 5 - 10
  seq 5 deny 100.100.1.0/24 (hit count: 5)
  seq 6 deny 200.200.1.0/24 (hit count: 1)
  seq 7 deny 200.200.2.0/24 (hit count: 1)
  seq 10 permit 0.0.0.0/0 le 32 (hit count: 132)
FTOS#
```

show ip prefix-list summary

Display a summary of the configured prefix lists.

S5000

Syntax `show ip prefix-list summary [`*`prefix-name`*`]`

Parameters

prefix-name	(OPTIONAL) Enter a text string as the name of the prefix list, up to 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip prefix summary
Prefix-list with the last deletion/insertion: test
ip prefix-list test:
count: 3, range entries: 1, sequences: 5 - 15
ip prefix-list test1:
count: 2, range entries: 2, sequences: 5 - 10
ip prefix-list test2:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test3:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test4:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test5:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test6:
count: 1, range entries: 1, sequences: 5 - 5
FTOS#
```

Route Map Commands

When you create an access-list without any rule and then apply it to an interface, the ACL behavior reflects implicit permit.

The following commands allow you to configure route maps and their redistribution criteria.

continue

Configure a route-map to go to a route-map entry with a higher sequence number.

S5000

Syntax `continue [sequence-number]`

Parameters

sequence-number	(OPTIONAL) Enter the route map sequence number. The range is 1 to 65535.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `continue` feature allows movement from one route-map entry to a specific route-map entry (the sequence number). If you do not specify the sequence number, the `continue` feature simply moves to the next sequence number (also known as an implied continue). If a match clause exists, the `continue` feature executes only after a successful match occurs. If there are no successful matches, the `continue` feature is ignored.

Match clause with Continue clause

The `continue` feature can exist without a match clause. A continue clause without a match clause executes and jumps to the specified route-map entry.

With a match clause and a continue clause, the match clause executes first and the continue clause next in a specified route map entry. The continue clause launches only after a successful match. The behavior is:

- A successful match with a continue clause, the route map executes the set clauses and then goes to the specified route map entry upon execution of the continue clause.
- If the next route map entry contains a continue clause, the route map executes the continue clause if a successful match occurs.
- If the next route map entry does not contain a continue clause, the route map evaluates normally. If a match does not occur, the route map does not continue and falls through to the next sequence number, if one exists.

Set Clause with Continue Clause

If the route-map entry contains sets with the continue clause, set actions are performed first then the continue clause jumps to the specified route map entry.

- If a set action occurs in the first route map entry and then the same set action occurs with a different value in a subsequent route map entry, the last set of actions overrides the previous set of actions with the same `set` command.
- If `set community additive` and `set as-path prepend` are configure, the communities and AS numbers are prepended.

Related Commands

set community — specifies a COMMUNITY attribute.

set as-path — configures a filter to modify the AS path.

description

Add a description to this route map.

S5000

Syntax	`description {description}`
Parameters	***description*** — Enter a description to identify the route map (80 characters maximum).
Defaults	none
Command Modes	ROUTE-MAP
Command History	**Version 9.0(1.3)** — Introduced on the S5000.
Related Commands	route-map – enables a route map.

match as-path

Configure a filter to match routes that have a certain AS number in their BGP path.

S5000

Syntax	`match as-path as-path-name`
Parameters	***as-path-name*** — Enter the name of an established AS-PATH ACL, up to 140 characters.
Defaults	Not configured.
Command Modes	ROUTE-MAP
Command History	**Version 9.0(1.3)** — Introduced on the S5000.
Related Commands	set as-path – adds information to the BGP AS_PATH attribute.

match community

Configure a filter to match routes that have a certain COMMUNITY attribute in their BGP path.

S5000

Syntax	`match community` *`community-list-name`* `[exact]`
Parameters	

community-list-name	Enter the name of a configured community list.
exact	(OPTIONAL) Enter the keywords `exact` to process only those routes with this community list name.

Defaults	Not configured.
Command Modes	ROUTE-MAP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	ip community-list – configures an Community Access list. set community – specifies a COMMUNITY attribute. neighbor send-community – sends COMMUNITY attribute to peer or peer group.

match interface

Configure a filter to match routes whose next hop is on the interface specified.

S5000

Syntax	`match interface` *`interface`* To remove a match, use the `no match interface` *`interface`* command.
Parameters	

interface

Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` and then enter the slot/port information.
- For the loopback interface, enter the keyword `loopback` and then enter a number from zero (0) to 16383.
- For a Port Channel interface, enter the keyword `port-channel` and then enter a number. The range is 1 to 128.
- For a VLAN, enter the keyword `vlan` and then enter a number from 1 to 4094.

Defaults	Not configured.
Command Modes	ROUTE-MAP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	match ip address – redistributes routes that match an IP address. match ip next-hop – redistributes routes that match the next-hop IP address. match ip route-source – redistributes routes that match routes advertised by other routers. match metric – redistributes routes that match a specific metric. match route-type – redistributes routes that match a route type. match tag – redistributes routes that match a specific tag.

match ip address

Configure a filter to match routes based on IP addresses specified in an access list.

S5000

Syntax	`match ip address prefix-list-name`
Parameters	***prefix-list-name*** Enter the name of configured prefix list, up to 140 characters.
Defaults	Not configured.
Command Modes	ROUTE-MAP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	match interface – redistributes routes that match the next-hop interface. match ip next-hop – redistributes routes that match the next-hop IP address. match ip route-source – redistributes routes that match routes advertised by other routers. match metric – redistributes routes that match a specific metric. match route-type – redistributes routes that match a route type. match tag – redistributes routes that match a specific tag.

match ip next-hop

Configure a filter to match based on the next-hop IP addresses specified in an IP access list or IP prefix list.

S5000

Syntax

```
match ip next-hop {access-list | prefix-list prefix-list-name}
```

Parameters

access-list-name	Enter the name of a configured IP access list, up to 140 characters.
prefix-list *prefix-list-name*	Enter the keywords `prefix-list` and then enter the name of configured prefix list, up 10 140 characters.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

match interface – redistributes routes that match the next-hop interface.

match ip address – redistributes routes that match an IP address.

match ip route-source – redistributes routes that match routes advertised by other routers.

match metric – redistributes routes that match a specific metric.

match route-type – redistributes routes that match a route type.

match tag – redistributes routes that match a specific tag.

match ip route-source

Configure a filter to match based on the routes advertised by routes specified in IP access lists or IP prefix lists.

S5000

Syntax

```
match ip route-source {access-list | prefix-list prefix-list-
name}
```

Parameters

access-list-name	Enter the name of a configured IP access list, up to 140 characters.
prefix-list *prefix-list-name*	Enter the keywords `prefix-list` and then enter the name of configured prefix list, up to 140 characters.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

- match interface – redistributes routes that match the next-hop interface.
- match ip address – redistributes routes that match an IP address.
- match ip next-hop – redistributes routes that match the next-hop IP address.
- match metric – redistributes routes that match a specific metric.
- match route-type – redistributes routes that match a route type.
- match tag – redistributes routes that match a specific tag.

match metric

Configure a filter to match on a specified value.

S5000

Syntax

```
match metric metric-value
```

Parameters

metric-value	Enter a value to match. The range is zero (0)–4294967295.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

- match interface – redistributes routes that match the next-hop interface.
- match ip address – redistributes routes that match an IP address.
- match ip next-hop – redistributes routes that match the next-hop IP address.
- match ip route-source – redistributes routes that match routes advertised by other routers.
- match route-type – redistributes routes that match a route type.
- match tag – redistributes routes that match a specific tag.

match route-type

Configure a filter to match routes based on the how the route is defined.

S5000

Syntax

```
match route-type {external [type-1 | type-2] | internal |
level-1 | level-2 | local}
```

Parameters

external [type-1|type-2]	Enter the keyword `external` and then enter either type-1 or type-2 to match only on OSPF Type 1 routes or OSPF Type 2 routes.
internal	Enter the keyword `internal` to match only on routes generated within OSPF areas.
level-1	Enter the keyword `level-1` to match IS-IS Level 1 routes.
level-2	Enter the keyword `level-2` to match IS-IS Level 2 routes.
local	Enter the keyword `local` to match only on routes generated within the switch.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

match interface – redistributes routes that match the next-hop interface.

match ip address – redistributes routes that match an IP address.

match ip next-hop – redistributes routes that match the next-hop IP address.

match ip route-source – redistributes routes that match routes advertised by other routers.

match metric – redistributes routes that match a specific metric.

match tag – redistributes routes that match a specific tag.

match tag

Configure a filter to redistribute only routes that match a specified tag value.

S5000

Syntax `match tag` *`tag-value`*

Parameters

tag-value	Enter a value as the tag on which to match. The range is zero (0) to 4294967295.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

match interface – redistributes routes that match the next-hop interface.

match ip address – redistributes routes that match an IP address.

match ip next-hop – redistributes routes that match the next-hop IP address.

match ip route-source – redistributes routes that match routes advertised by other routers.

match metric – redistributes routes that match a specific metric.

match route-type – redistributes routes that match a route type.

route-map

Enable a route map statement and configure its action and sequence number. This command also places you in ROUTE-MAP mode.

S5000

Syntax

```
route-map map-name [permit | deny] [sequence-number]
```

Parameters

map-name	Enter a text string of up to 140 characters to name the route map for easy identification.
permit	(OPTIONAL) Enter the keyword `permit` to set the route map default as permit. If you do not specify a keyword, the default is `permit`.
deny	(OPTIONAL) Enter the keyword `deny` to set the route map default as deny.
sequence-number	(OPTIONAL) Enter a number to identify the route map for editing and sequencing with other route maps. You are prompted for a sequence number if there are multiple instances of the route map. The range is 1 to 65535.

Defaults

Not configured.

If you do not define a keyword (`permit` or `deny`) for the route map, the `permit` action is the default.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use caution when you delete route maps because if you do not specify a sequence number, all route maps with the same *map-name* are deleted when you use the `no route-map map-name` command.

Example

```
FTOS(conf)#route-map dempsey
FTOS(config-route-map)#
```

Related Commands

show config – displays the current configuration.

set as-path

Configure a filter to modify the AS path for border gateway protocol (BGP) routes.

S5000

Syntax

`set as-path prepend` *`as-number`* `[...` *`as-number`*`]`

Parameters

prepend *as-number*	Enter the keyword `prepend` and then enter up to eight AS numbers to be inserted into the BGP path information. The range is 1 to 65535.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can prepend up to eight AS numbers to a BGP route.

This command influences best path selection in BGP by inserting a tag or AS number into the AS_PATH attribute.

Related Commands

match as-path – redistributes routes that match an AS-PATH attribute.

ip as-path access-list – configures an AS-PATH access list.

neighbor filter-list – configures a BGP filter based on the AS-PATH attribute.

show ip community-lists – displays configured IP Community access lists.

set automatic-tag

Configure a filter to automatically compute the tag value of the route.

S5000

Syntax

`set automatic-tag`

To return to the default, enter `no set automatic-tag`.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

set level – specify the OSPF area for route redistribution.

set metric – specify the metric value assigned to redistributed routes.

set metric-type – specify the metric type assigned to redistributed routes.

set tag – specify the tag assigned to redistributed routes.

set comm-list delete

Configure a filter to remove the specified community list from the BGP route's COMMUNITY attribute.

S5000

Syntax

`set comm-list` *`community-list-name`* `delete`

Parameters

community-list-name	Enter the name of an established Community list, up to 140 characters.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The community list used in the `set comm-list delete` command must be configured so that each filter contains only one community. For example, the filter `deny 100:12` is acceptable, but the filter `deny 120:13 140:33` results in an error.

If the `set comm-list delete` command and the `set community` command are configured in the same route map sequence, the deletion command (`set comm-list delete`) is processed before the insertion command (`set community`).

Related Commands

ip community-list – configures community access list.

match community – redistributes routes that match the COMMUNITY attribute.

set community – specifies a COMMUNITY attribute.

set community

Allows you to assign a BGP COMMUNITY attribute.

S5000

Syntax

```
set community {community-number | local-as | no-advertise | no-
export | none} [additive]
```

To delete a BGP COMMUNITY attribute assignment, use the `no set community {community-number | local-as | no-advertise | no-export | none}` command.

Parameters

community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system.
local-AS	Enter the keywords `local-AS` to drop all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords `no-advertise` to drop all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords `no-export` to drop all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.
none	Enter the keyword `none` to remove the community attribute from routes meeting the route map criteria.
additive	(OPTIONAL) Enter the keyword `additive` to add the communities to already existing communities.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

ip community-list – configures community access list.

match community – redistributes routes that match the COMMUNITY attribute.

neighbor send-community – assigns the COMMUNITY attribute.

show ip bgp community – displays BGP community groups.

show ip community-lists – displays configured Community access lists.

set level

Configure a filter to specify the IS-IS level or OSPF area to which matched routes are redistributed.

S5000

Syntax

```
set level {backbone | level-1 | level-1-2 | level-2 | stub-
area}
```

Parameters

backbone	Enter the keyword `backbone` to redistribute matched routes to the OSPF backbone area (area 0.0.0.0).
level-1	Enter the keyword `level-1` to redistribute matched routes to IS-IS Level 1.
level-1-2	Enter the keyword `level-1-2` to redistribute matched routes to IS-IS Level 1 and Level 2.
level-2	Enter the keyword `level-2` to redistribute matched routes to IS-IS Level 2.
stub-area	Enter the keyword `stub` to redistributed matched routes to OSPF stub areas.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

set automatic-tag – computes the tag value of the route.

set metric – specifies the metric value assigned to redistributed routes.

set metric-type – specifies the metric type assigned to redistributed routes.

set tag – specifies the tag assigned to redistributed routes.

set local-preference

Configure a filter to set the BGP LOCAL_PREF attribute for routers within the local autonomous system.

S5000

Syntax `set local-preference` *`value`*

Parameters

value	Enter a number as the LOCAL_PREF attribute value. The range is 0 to 4294967295.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `set local-preference` command changes the LOCAL_PREF attribute for routes meeting the route map criteria. To change the LOCAL_PREF for all routes, use the `bgp default local-preference` command.

Related Commands	bgp default local-preference – changes the default LOCAL_PREF attribute for all routes.

set metric

Configure a filter to assign a new metric to redistributed routes.

S5000

Syntax

```
set metric [+ | -] metric-value
```

To delete a setting, enter `no set metric`.

Parameters

+	(OPTIONAL) Enter + to add a metric-value to the redistributed routes.
-	(OPTIONAL) Enter – to subtract a metric-value from the redistributed routes.
metric-value	Enter a number as the new metric value. The range is zero (0) to 4294967295.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

set automatic-tag – computes the tag value of the route.

set level – specifies the OSPF area for route redistribution.

set metric-type – specifies the route type assigned to redistributed routes.

set tag – specifies the tag assigned to redistributed routes.

set metric-type

Configure a filter to assign a new route type for routes redistributed to OSPF.

S5000

Syntax

```
set metric-type {internal | external | type-1 | type-2}
```

Parameters

internal	Enter the keyword `internal` to assign the Interior Gateway Protocol metric of the next hop as the route’s BGP MULTI_EXIT_DES (MED) value.

	external	Enter the keyword `external` to assign the IS-IS external metric.
	type-1	Enter the keyword `type-1` to assign the OSPF Type 1 metric.
	type-2	Enter the keyword `type-2` to assign the OSPF Type 2 metric.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

set automatic-tag – computes the tag value of the route.

set level – specifies the OSPF area for route redistribution.

set metric – specifies the metric value assigned to redistributed routes.

set tag – specifies the tag assigned to redistributed routes.

set next-hop

Configure a filter to specify an IP address as the next hop.

S5000

Syntax `set next-hop ip-address`

Parameters

ip-address	Specify an IP address in dotted decimal format.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you configure the `set next-hop` command, its configuration takes precedence over the `neighbor next-hop-self` command in the ROUTER BGP mode.

If you configure the `set next-hop` command with the interface's IP address (either Loopback or physical), the software declares the route unreachable.

Related Commands

match ip next-hop – redistributes routes that match the next-hop IP address.

neighbor next-hop-self – configures the routers as the next hop for a BGP neighbor.

set origin

Configure a filter to manipulate the BGP ORIGIN attribute.

S5000

Syntax `set origin {igp | egp | incomplete}`

Parameters

egp	Enter the keyword `egp` to set routes originating from outside the local AS.
igp	Enter the keyword `igp` to set routes originating within the same AS.
incomplete	Enter the keyword `incomplete` to set routes with incomplete routing information.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

set tag

Configure a filter to specify a tag for redistributed routes.

S5000

Syntax `set tag tag-value`

Parameters

tag-value	Enter a number as the tag. The range is zero (0) to 4294967295.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

set automatic-tag – computes the tag value of the route.

set level – specifies the OSPF area for route redistribution.

set metric – specifies the metric value assigned to redistributed routes.

set metric-type – specifies the route type assigned to redistributed routes.

set weight

Configure a filter to add a non-RFC compliant attribute to the BGP route to assist with route selection.

S5000

Syntax `set weight weight`

Parameters

weight	Enter a number as the weight to be used by the route meeting the route map specification. The range is 0 to 65535. The default is router-originated = **32768** and all other routes = **0**. When there are multiple routes to the same destination, routes with a higher weight are preferred.

Defaults router-originated = **32768**; all other routes = **0**

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If you do not use the `set weight` command, router-originated paths have a weight attribute of 32768 and all other paths have a weight attribute of zero.

show config

Display the current route map configuration.

S5000

Syntax `show config`

Command Modes ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(config-route-map)#show config
!
route-map hopper permit 10
FTOS(config-route-map)#
```

show route-map

Display the current route map configurations.

S5000

Syntax `show route-map [map-name]`

Parameters

map-name	(OPTIONAL) Enter the name of a configured route map, up to 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show route-map
route-map firpo, permit, sequence 10
 Match clauses:
 Set clauses:
  tag 34
FTOS#
```

Related Commands route-map – configures a route map.

AS-Path Commands

The following commands configure AS-Path ACLs.

ip as-path access-list

Enter AS-PATH ACL mode and configure an access control list based on the BGP AS_PATH attribute.

S5000

Syntax `ip as-path access-list as-path-name`

Parameters

as-path-name	Enter the access-list name, up to 140 characters.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `match as-path` or `neighbor filter-list` commands to apply the AS-PATH ACL to BGP routes.

Example

```
FTOS(conf)#ip as-path access-list TestPath
FTOS(config-as-path)#
```

Related Commands

match as-path – matches on routes contain a specific AS-PATH.

neighbor filter-list – configures filter based on AS-PATH information.

show ip as-path-access-lists

Display the all AS-PATH access lists configured on the S5000.

S5000

Syntax

`show ip as-path-access-lists`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip as-path-access-lists
ip as-path access-list 1
 permit ^$
 permit ^\(.*\)$
 deny .*
ip as-path access-list 91
 permit ^$
 deny .*
 permit ^\(.*\)$
FTOS#
```

IP Community List Commands

IP Community List commands are supported on the S5000.

ip community-list

Enter COMMUNITY-LIST mode and create an IP community-list for BGP.

S5000

Syntax	`ip community-list` *`comm-list-name`* To delete a community-list, use the `no ip community-list` *`comm-list-name`* command.
Parameters	***comm-list-name*** — Enter a text string as the name of the community-list, up to 140 characters.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

Example

```
FTOS(conf)#ip community-list TestComList
FTOS(config-community-list)#
```

show ip community-lists

Display configured IP community lists in alphabetic order.

S5000

Syntax	`show ip community-lists [`*`name`*`]`
Parameters	***name*** — (OPTIONAL) Enter the name of the standard or extended IP community list, up to 140 characters.
Command Modes	• EXEC • EXEC Privilege
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

Example

```
FTOS#show ip community-lists
ip community-list standard 1
 deny 701:20
 deny 702:20
 deny 703:20
 deny 704:20
 deny 705:20
 deny 14551:20
 deny 701:112
 deny 702:112
 deny 703:112
 deny 704:112
 deny 705:112
 deny 14551:112
 deny 701:666
 deny 702:666
 deny 703:666
 deny 704:666
 deny 705:666
 deny 14551:666
FTOS#
```

9

Bidirectional Forwarding Detection (BFD)

Bidirectional forwarding detection (BFD) is a detection protocol that provides fast forwarding path failure detection.

FTOS is based on the standards specified in the IETF Draft draft-ietf-bfd-base-03 and supports BFD on all Layer 3 physical interfaces including virtual local area network (VLAN) interfaces, and port-channels.

BFD is supported on the S5000.

bfd all-neighbors

Enable BFD sessions with all neighbors discovered by Layer 3 protocols intermediate system to intermediate system (IS-IS), open shortest path first (OSPF), or border gateway protocol (BGP) on router interfaces, and (optionally) reconfigure the default timer values.

S5000

Syntax

`bfd all-neighbors [interval` *`interval`* `min_rx` *`min_rx`* `multiplier` *`value`* `role {active | passive}]`

Parameters

interval ***milliseconds***	(OPTIONAL) Enter the keywords `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is 50 to 1000. The default is **100**.
min_rx ***milliseconds***	Enter the keywords `min_rx` to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is 50 to 100. The default is **100**.
multiplier ***value***	Enter the keywords `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is 3 to 50. The default is **3**.
role [active | passive]	Enter the role that the local system assumes: • `Active`—The active system initiates the BFD session. Both systems can be active for the same session. • `Passive`—The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default it **active**.

Defaults See Parameters

Command Modes

ROUTER OSPF

ROUTER BGP

ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced BFD for BGP on the S5000.

Usage Information

All neighbors inherit the timer values configured with the `bfd all-neighbors` command except in the following cases:

- Timer values configured with the `isis bfd all-neighbors` command in INTERFACE mode override timer values configured with the `bfd all-neighbors` command. Likewise, using the `no bfd all-neighbors` command does not disable BFD on an interface if BFD is explicitly enabled using the `isis bfd all-neighbors` command.
- Neighbors that have been explicitly enabled or disabled for a BFD session with the `bfd neighbor` or `neighbor bfd disable` commands in ROUTER BGP mode do not inherit the global BFD enable/ disable values configured with the `bfd all-neighbors` command or configured for the peer group to which a neighbor belongs. The neighbors inherit only the global timer values (configured with the `bfd all-neighbors` command).

Related Commands

show bfd neighbors – displays BFD neighbor information on all interfaces or a specified interface.

bfd neighbor – explicitly enables a BFD session with a BGP neighbor or a BGP peer group.

neighbor bfd disable – explicitly disables a BFD session with a BGP neighbor or a BGP peer group.

bfd enable (Configuration)

Enable BFD on all interfaces.

S5000

Syntax

`bfd enable`

Disable BFD using the `no bfd enable` command.

Defaults

BFD is disabled by default.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

bfd enable (Interface)

Enable BFD on an interface.

S5000

Syntax	`bfd enable`
Defaults	BFD is enabled on all interfaces when you enable BFD from CONFIGURATION mode.
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

bfd protocol-liveness

Enable the BFD protocol liveness feature.

S5000

Syntax	`bfd protocol-liveness`
Defaults	Disabled
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Protocol Liveness is a feature that notifies the BFD Manager when a client protocol (for example, OSPF and ISIS) is disabled. When a client is disabled, all BFD sessions for that protocol are torn down. Neighbors on the remote system receive an Admin Down control packet and are placed in the Down state. Peer routers might take corrective action by choosing alternative paths for the routes that originally pointed to this router.

neighbor bfd

Explicitly enable a BFD session with a BGP neighbor or a BGP peer group.

S5000

Syntax `neighbor {`*`ip-address`*` | `*`peer-group-name`*`} bfd`

Parameters

ip-address	Enter the IP address of the BGP neighbor that you want to explicitly enable for BFD sessions in dotted decimal format (A.B.C.D).

peer-group-name	Enter the name of the peer group that you want to explicitly enable for BFD sessions.

Defaults none

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you enable a BFD session with a specified BGP neighbor or peer group using the `bfd neighbor` command, the default BFD session parameters are used (interval: **100** milliseconds, min_rx: **100** milliseconds, multiplier: **3** packets, and role: **active**) if you have not specified parameters with the `bfd all-neighbors` command.

When you explicitly enable a BGP neighbor for a BFD session with the `bfd neighbor` command:

- The neighbor does not inherit the global BFD enable values configured with the `bfd all-neighbors` command or configured for the peer group to which the neighbor belongs.
- The neighbor only inherits the global timer values configured with the `bfd all-neighbors` command: interval, min_rx, and multiplier.

Related Commands

bfd all-neighbors – enables BFD sessions with all neighbors discovered by Layer 3 protocols.

neighbor bfd disable – explicitly disables a BFD session with a BGP neighbor or a BGP peer group.

show bfd neighbors – displays the BFD neighbor information on all interfaces or a specified interface.

neighbor bfd disable

Explicitly disable a BFD session with a BGP neighbor or a BGP peer group.

S5000

Syntax `neighbor {ip-address | peer-group-name} bfd disable`

Parameters

ip-address	Enter the IP address of the BGP neighbor that you want to explicitly disable for BFD sessions in dotted decimal format (A.B.C.D).
peer-group-name	Enter the name of the peer group that you want to explicitly disable for BFD sessions.

Defaults none

Command Modes ROUTER BGP

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Usage Information

When you explicitly disable a BGP neighbor for a BFD session with the `neighbor bfd disable` command:

- The neighbor does not inherit the global BFD disable values configured with the `bfd all-neighbors` command or configured for the peer group to which the neighbor belongs.
- The neighbor only inherits the global timer values configured with the `bfd all-neighbors` command: interval, min_rx, and multiplier.

When you remove the disabled state of a BFD for BGP session with a specified neighbor by entering the `no neighbor bfd disable` command, the BGP link with the neighbor returns to normal operation and uses the BFD session parameters globally configured with the `bfd all-neighbors` command or configured for the peer group to which the neighbor belongs.

Related Commands

bfd all-neighbors – enables BFD sessions with all neighbors discovered by Layer 3 protocols.

bfd neighbor – explicitly enables a BFD session with a BGP neighbor or a BGP peer group.

show bfd neighbors – displays the BFD neighbor information on all interfaces or a specified interface.

show bfd neighbors

Display BFD neighbor information on all interfaces or a specified interface.

S5000

Syntax

`show bfd neighbors interface-type slot/port [detail]`

Parameters

interface-type slot/port	Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
detail	(OPTIONAL) Enter the keyword `detail` to view detailed information about BFD neighbors.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show bfd neighbors

*     - Active session role
Ad Dn - Admin Down
B     - BGP
C     - CLI
I     - ISIS
O     - OSPF
R     - Static Route (RTM)

  LocalAddr  RemoteAddr  Interface State Rx-int Tx-int Mult
Clients
* 10.1.3.2   10.1.3.1    Te 1/3    Up    300    250    3    C
```

Example (Detail)

```
FTOS#show bfd neighbors detail

Session Discriminator: 1
Neighbor Discriminator: 1
Local Addr: 10.1.3.2
Local MAC Addr: 00:01:e8:02:15:0e
Remote Addr: 10.1.3.1
Remote MAC Addr: 00:01:e8:27:2b:f1
Int: TenGigabitEthernet 1/3
State: Up
Configured parameters:
 TX: 100ms, RX: 100ms, Multiplier: 3
Neighbor parameters:
 TX: 250ms, RX: 300ms, Multiplier: 4
Actual parameters:
 TX: 300ms, RX: 250ms, Multiplier: 3
Role: Active
Delete session on Down: False
Client Registered: CLI
Uptime: 00:02:04
Statistics:
 Number of packets received from neighbor: 376
 Number of packets sent to neighbor: 314
 Number of state changes: 2
 Number of messages from IFA about port state change: 0
 Number of messages communicated b/w Manager and Agent: 6
FTOS#
```

Related Commands

bfd neighbor – establishes a BFD session with a neighbor.

bfd all-neighbors – establishes BFD sessions with all neighbors discovered by the IS-IS protocol or OSPF protocol out of all interfaces.

10

Border Gateway Protocol IPv4 (BGPv4)

BGP is an external gateway protocol that transmits interdomain routing information within and between autonomous systems (AS). BGP version 4 (BGPv4) supports classless inter-domain routing (CIDR) and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically sent messages to update those routing tables.

FTOS supports BGPv4 on the S5000 switch:

NOTE: For more information about configuring the border gateway protocol (BGP), refer to the BGP chapter in the *FTOS Configuration Guide*.

This chapter contains the following sections:

- BGPv4 Commands
- MBGP Commands
- BGP Extended Communities (RFC 4360)

BGPv4 Commands

Border Gateway Protocol (BGP) is an external gateway protocol that transmits interdomain routing information within and between Autonomous Systems (AS). BGP version 4 (BGPv4) supports classless interdomain routing (CIDR) and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

address-family

Enable the IPv4 multicast or the IPv6 address family.

S5000

Syntax `address-family [ipv4 multicast| ipv6unicast]`

Parameters

ipv4 multicast	Enter BGPv4 multicast mode.
ipv6 unicast	Enter BGPv6 mode.

Defaults Not configured.

Command Modes ROUTER BGP

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

aggregate-address

Summarize a range of prefixes to minimize the number of entries in the routing table.

S5000

Syntax

```
aggregate-address ip-address mask [advertise-map map-name] [as-set] [attribute-map map-name] [summary-only] [suppress-map map-name]
```

Parameters

ip-address mask	Enter the IP address and mask of the route to be the aggregate address. Enter the IP address in dotted decimal format (A.B.C.D) and mask in /prefix format (/x).
advertise-map *map-name*	(OPTIONAL) Enter the keywords `advertise-map` followed by the name of a configured route map to set filters for advertising an aggregate route.
as-set	(OPTIONAL) Enter the keyword `as-set` to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.
attribute-map *map-name*	(OPTIONAL) Enter the keywords `attribute-map` followed by the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
summary-only	(OPTIONAL) Enter the keyword `summary-only` to advertise only the aggregate address. Specific routes are not advertised.
suppress-map *map-name*	(OPTIONAL) Enter the keywords `suppress-map` followed by the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

Defaults

Not configured.

Command Modes

- ROUTER BGP ADDRESS FAMILY
- ROUTER BGP ADDRESS FAMILY IPv6

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Usage Information

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

If routes within the aggregate are constantly changing, do not add the `as-set` parameter to the aggregate as the aggregate flaps to keep track of the changes in the AS_PATH.

In route maps used in the `suppress-map` parameter, routes meeting the `deny` clause are not suppress; in other words, they are allowed. The opposite is also true: routes meeting the `permit` clause are suppressed.

If the route is injected via the `network` command, that route still appears in the routing table if the `summary-only` parameter is configured in the `aggregate-address` command.

The `summary-only` parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the `neighbor distribute-list` command.

In the `show ip bgp` command, aggregates contain an 'a' in the first column and routes suppressed by the aggregate contain an 's' in the first column.

bgp add-path

Allow the advertisement of multiple paths for the same address prefix without the new paths replacing any previous ones.

S5000

Syntax

```
bgp add-path [send | receive | both] count
```

Parameters

send	Enter the keyword `send` to indicate that the system will send multiple paths to peers.
receive	Enter the keyword `receive` to indicate that the system will accept multiple paths from peers.
both	Enter the keyword `both` to indicate that the system will send and accept multiple paths from peers.
count	Enter the number paths supported. The range is 2 to 64.

Defaults Disabled

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands neighbor add-path – specifies that this neighbor/peer group can send/receive multiple path advertisements.

bgp always-compare-med

Allows you to enable comparison of the MULTI_EXIT_DISC (MED) attributes in the paths from different external ASs.

S5000

Syntax

`bgp always-compare-med`

To disable comparison of MED, enter `no bgp always-compare-med`.

Defaults

Disabled (that is, the software only compares MEDs from neighbors within the same AS).

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Any update without a MED attribute is the least preferred route.

If you enable this command, use the `clear ip bgp *` command to recompute the best path.

bgp asnotation

Allows you to implement a method for AS number representation in the command line interface (CLI).

S5000

Syntax

`bgp asnotation [`*`asplain`*` | `*`asdot+`*` | `*`asdot`*`]`

To disable a dot or dot+ representation and return to ASPLAIN, enter the `no bgp asnotation` command.

Defaults

asplain

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Before enabling this feature, you must enable the `enable bgp four-octet-as-support`command. If you disable the `four-octect-support` command after using dot or dot+ format, the AS numbers revert to asplain text.

When you apply an asnotation, it is reflected in the running-configuration. If you change the notation type, the running-config updates dynamically and the new notation showns.

Example

```
FTOS(conf)#router bgp 1
FTOS(conf-router_bgp)#bgp asnotation asdot
FTOS(conf-router_bgp)#ex
FTOS(conf)#do show run | grep bgp

router bgp 1
  bgp four-octet-as-support
  bgp asnotation asdot

FTOS(conf)#router bgp 1
FTOS(conf-router_bgp)#bgp asnotation asdot+
FTOS(conf-router_bgp)#ex

FTOS(conf)#do show run | grep bgp
router bgp 1
  bgp four-octet-as-support
  bgp asnotation asdot+

FTOS(conf)#router bgp 1
FTOS(conf-router_bgp)#bgp asnotation asplain
FTOS(conf-router_bgp)#ex
FTOS(conf)#do show run |grep bgp
router bgp 1
  bgp four-octet-as-support

FTOS(conf)#
```

Related Commands

bgp four-octet-as-support – enables 4-byte support for the BGP process.

bgp bestpath as-path ignore

Ignore the AS PATH in BGP best path calculations.

S5000

Syntax

`bgp bestpath as-path ignore`

To return to the default, enter the `no bgp bestpath as-path ignore` command.

Defaults

Disabled (that is, the software considers the AS_PATH when choosing a route as best).

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you enable this command, use the `clear ip bgp *` command to recompute the best path.

bgp bestpath as-path multipath-relax

Include prefixes received from different AS paths during multipath calculation.

S5000

Syntax

`bgp bestpath as-path multipath-relax`

To return to the default BGP routing process, use the `no bgp bestpath as-path multipath-relax` command.

Defaults Disabled

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The `bestpath router bgp configuration mode` command changes the default bestpath selection algorithm. The `multipath-relax` option allows load-sharing across providers with different (but equal-length) autonomous system paths. Without this option, ECMP expects the AS paths to be identical for load-sharing.

bgp bestpath med confed

Enable MULTI_EXIT_DISC (MED) attribute comparison on paths learned from BGP confederations.

S5000

Syntax `bgp bestpath med confed`

To disable MED comparison on BGP confederation paths, enter the `no bgp bestpath med confed` command.

Defaults Disabled

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The software compares the MEDs only if the path contains no external autonomous system numbers. If you enable this command, use the `clear ip bgp *` command to recompute the best path.

bgp bestpath med missing-as-best

During path selection, indicate preference to paths with missing MED (MULTI_EXIT_DISC) over those paths with an advertised MED attribute.

S5000

Syntax `bgp bestpath med missing-as-best`

To return to the default selection, use the `no bgp bestpath med missing-as-best` command.

Defaults	Disabled
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	The MED is a 4-byte unsigned integer value and the default behavior is to assume a missing MED as 4294967295. This command causes a missing MED to be treated as 0. During path selection, paths with a lower MED are preferred over those with a higher MED.

bgp bestpath router-id ignore

Do not compare router-id information for external paths during best path selection.

S5000

Syntax	`bgp bestpath router-id ignore` To return to the default selection, use the `no bgp bestpath router-id ignore` command.
Defaults	Disabled
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Configuring this option retains the current best-path. When sessions are subsequently reset, the oldest received path is chosen as the best-path.

bgp client-to-client reflection

Allows you to enable route reflection between clients in a cluster.

S5000

Syntax	`bgp client-to-client reflection` To disable client-to-client reflection, use the `no bgp client-to-client reflection` command.
Defaults	Enabled when a route reflector is configured.
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Usage Information

Route reflection to clients is not necessary if all client routers are fully meshed.

Related Commands

bgp cluster-id – assigns an ID to a BGP cluster with two or more route reflectors.

neighbor route-reflector-client – configures a route reflector and clients.

bgp cluster-id

Assign a cluster ID to a BGP cluster with more than one route reflector.

S5000

Syntax

`bgp cluster-id {ip-address | number}`

To delete a cluster ID, use the `no bgp cluster-id {ip-address | number}` command.

Parameters

ip-address	Enter an IP address as the route reflector cluster ID.
number	Enter a route reflector cluster ID as a number from 1 to 4294967295.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When a BGP cluster contains only one route reflector, the cluster ID is the route reflector's router ID. For redundancy, a BGP cluster may contain two or more route reflectors. Assign a cluster ID with the `bgp cluster-id` command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster.

The default format for displaying the cluster-id is dotted decimal, but if you enter the cluster-id as an integer, it is displayed as an integer.

Related Commands

bgp client-to-client reflection – enables route reflection between the route reflector and clients.

neighbor route-reflector-client – configures a route reflector and clients.

show ip bgp cluster-list – views paths with a cluster ID.

bgp confederation identifier

Configure an identifier for a BGP confederation.

S5000

Syntax

`bgp confederation identifier as-number`

To delete a BGP confederation identifier, use the `no bgp confederation identifier as-number` command.

Parameters

as-number	Enter the AS number. The range is 0 to 65535 (2-byte), 1 to 4294967295 (4-byte), or 0.1 to 65535.65535 (dotted format).

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must configure your system to accept 4-byte formats before entering a 4-byte AS number. All the routers in the Confederation must be 4– or 2-byte identified routers. You cannot mix them.

The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation.

FTOS accepts confederation EBGP peers without a LOCAL_PREF attribute. The software sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.

Related Commands

bgp four-octet-as-support – enables 4-byte support for the BGP process.

bgp confederation peers

Specify the autonomous systems (ASs) that belong to the BGP confederation.

S5000

Syntax

`bgp confederation peers as-number [...as-number]`

To return to the default, use the `no bgp confederation peers` command.

Parameters

as-number	Enter the AS number. The range is 0 to 65535 (2-byte), 1 to 4294967295 (4-byte), or 0.1 to 65535.65535 (dotted format).
...as-number	(OPTIONAL) Enter up to 16 confederation numbers. The range is 0 to 65535 (2-byte), 1 to 4294967295 (4-byte), or 0.1 to 65535.65535 (dotted format).

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

All the routers in the Confederation must be 4- or 2-byte identified routers. You cannot mix them.

The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems.

After specifying autonomous systems numbers for the BGP confederation, recycle the peers to update their configuration.

Related Commands

bgp confederation identifier – configures a confederation ID.

bgp four-octet-as-support – enables 4-byte support for the BGP process.

bgp dampening

Enable BGP route dampening and configure the dampening parameters.

S5000

Syntax

`bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]`

To disable route dampening, use the `no bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]` command.

Parameters

half-life	(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half after the half-life period expires. The range is 1 to 45. The default is **15 minutes**.
reuse	(OPTIONAL) Enter a number as the reuse value, which is compared to the flapping route's Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed). The range is 1 to 20000. The default is **750**.
suppress	(OPTIONAL) Enter a number as the suppress value, which is compared to the flapping route's Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed). The range is 1 to 20000. The default is **2000**.
max-suppress-time	(OPTIONAL) Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value. The range is 1 to 255. The default is **60 minutes**.

route-map *map-name*	(OPTIONAL) Enter the keyword `route-map` followed by the name of a configured route map. Only `match` commands in the configured route map are supported.

Defaults Disabled.

Command Modes ROUTER-BGP-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If you enter the `bgp dampening` command, the default values for *`half-life`*, *`reuse`*, *`suppress`*, and *`max-suppress-time`* are applied. The parameters are position-dependent; therefore, if you configure one parameter, you must configure the parameters in the order they appear in the CLI.

Related Commands show ip bgp dampened-paths – views the BGP paths.

bgp default local-preference

Change the default local preference value for routes exchanged between internal BGP peers.

S5000

Syntax `bgp default local-preference` *`value`*

To return to the default value, use the `no bgp default local-preference` command.

Parameters

value	Enter a number to assign to routes as the degree of preference for those routes. When routes are compared, the higher the degree of preference or local preference value, the more the route is preferred. The range is 0 to 4294967295. The default is **100**.

Defaults **100**

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The `bgp default local-preference` command setting is applied by all routers within the AS. To set the local preference for a specific route, use the `set local-preference` command in ROUTE-MAP mode.

Related Commands set local-preference – assigns a local preference value for a specific route.

bgp enforce-first-as

Disable (or enable) enforce-first-as check for updates received from EBGP peers.

S5000

Syntax	`bgp enforce-first-as` To turn off the default, use the `no bgp enforce-first-as` command.
Defaults	Enabled
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	This is enabled by default, that is for all updates received from EBGP peers, BGP ensures that the first AS of the first AS segment is always the AS of the peer. If not, the update is dropped and a counter is increments. Use the `show ip bgp neighbors` command to view the “failed enforce-first-as check” counter. If you disable the `enforce-first-as` command, it can be viewed using the `show ip protocols` command.
Related Commands	show ip bgp neighbors – views the information exchanged by BGP neighbors. show ip protocols – views information on routing protocols.

bgp fast-external-failover

Enable the fast external failover feature, which immediately resets the BGP session if a link to a directly connected external peer fails.

S5000

Syntax	`bgp fast-external-failover` To disable fast external failover, use the `no bgp fast-external-failover` command.
Defaults	Enabled
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	The `bgp fast-external-failover` command appears in the `show config` command output.

bgp four-octet-as-support

Enable 4-byte support for the BGP process.

S5000

Syntax	`bgp four-octet-as-support` To disable fast external fallover, use the `no bgp four-octet-as-support` command.
Defaults	Disabled (supports 2–byte format)
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Routers supporting 4-byte ASNs advertise that function in the OPEN message. The behavior of a 4-byte router is slightly different depending on whether it is speaking to a 2-byte router or a 4-byte router. When creating Confederations, all the routers in the Confederation must be 4- or 2-byte identified routers. You cannot mix them. Where the 2-byte format is 1 to 65535, the 4-byte format is 1 to 4294967295. Both formats are accepted and the advertisements reflect the entered format. For more information about using the 2- or 4-byte format, refer to the *FTOS Configuration Guide*.

bgp graceful-restart

Enable graceful restart on a BGP neighbor, a BGP node, or designate a local router to support graceful restart as a receiver only.

S5000

Syntax

`bgp graceful-restart [restart-time seconds] [stale-path-time seconds] [role receiver-only]`

To return to the default, use the `no bgp graceful-restart` command.

Parameters

restart-time ***seconds***	Enter the keyword `restart-time` followed by the maximum number of seconds needed to restart and bring-up all the peers. The range is 1 to 3600 seconds. The default is **120 seconds**.
stale-path-time ***seconds***	Enter the keyword `stale-path-time` followed by the maximum number of seconds to wait before restarting a peer's stale paths. The default is **360 seconds**.
role receiver-only	Enter the keyword `role receiver-only` to designate the local router to support graceful restart as a receiver only.

Defaults	as above
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	This feature is advertised to BGP neighbors through a capability advertisement. In Receiver Only mode, BGP saves the advertised routes of peers that support this capability when they restart. BGP graceful restart is active only when the neighbor becomes established. Otherwise it is disabled. Graceful-restart applies to all neighbors with established adjacency.

bgp log-neighbor-changes

Enable logging of BGP neighbor resets.

S5000

Syntax	`bgp log-neighbor-changes` To disable logging, use the `no bgp log-neighbor-changes` command.
Defaults	Enabled
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Use the `show logging` command in EXEC mode to view BGP neighbor resets. The `bgp log-neighbor-changes` command appears in the `show config` command output.
Related Commands	show logging – views logging settings and system messages logged to the system.

bgp non-deterministic-med

Compare MEDs of paths from different autonomous systems.

S5000

Syntax	`bgp non-deterministic-med` To return to the default, use the `no bgp non-deterministic-med` command.

Defaults	Disabled (that is, paths/routes for the same destination but from different ASs do not have their MEDs compared).
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	In Non-Deterministic mode, paths are compared in the order in which they arrive. This method can lead to FTOS choosing different best paths from a set of paths, depending on the order in which they are received from the neighbors because MED may or may not get compared between adjacent paths. In Deterministic mode (`no bgp non-deterministic-med`), FTOS compares MED between adjacent paths within an AS group because all paths in the AS group are from the same AS. When you change the path selection from Deterministic to Non-Deterministic, the path selection for the existing paths remains Deterministic until you enter the `clear ip bgp` command to clear existing paths.

bgp recursive-bgp-next-hop

Enable next-hop resolution through other routes learned by BGP.

S5000

Syntax	`bgp recursive-bgp-next-hop` To disable next-hop resolution, use the `no bgp recursive-bgp-next-hop` command.
Defaults	Enabled
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	This command is a *knob* to disable BGP next-hop resolution using BGP learned routes. During the next-hop resolution, only the first route that the next-hop resolves through is verified for the route's protocol source and is checked if the route is learned from BGP or not. The `clear ip bgp` command is required for this command to take effect and to keep the BGP database consistent. Execute the `clear ip bgp` command right after executing this command.
Related Commands	clear ip bgp – clears the ip bgp.

bgp regex-eval-optz-disable

Disables the Regex Performance engine that optimizes complex regular expression with BGP.

S5000

Syntax `bgp regex-eval-optz-disable`

To re-enable optimization engine, use the `no bgp regex-eval-optz-disable` command.

Defaults Enabled

Command Modes ROUTER BGP (conf-router_bgp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

BGP uses regular expressions (regex) to filter route information. In particular, the use of regular expressions to filter routes based on AS-PATHs and communities is quite common. In a large scale configuration, filtering millions of routes based on regular expressions can be quite CPU intensive, as a regular expression evaluation involves generation and evaluation of complex finite state machines.

BGP policies, containing regular expressions to match as-path and communities, tend to use a lot of CPU processing time, which in turn affects the BGP routing convergence. Additionally, the `show bgp` commands, which are filtered through regular expressions, use up CPU cycles particularly with large databases. The Regex Engine Performance Enhancement feature optimizes the CPU usage by caching and reusing regular expression evaluation results. This caching and reuse may be at the expense of processor memory.

Examples

```
FTOS(conf-router_bgp)#no bgp regex-eval-optz-disable
FTOS(conf-router_bgp)#do show ip protocols
Routing Protocol is "ospf 22222"
  Router ID is 2.2.2.2
  Area               Routing for Networks
  51                 10.10.10.0/00

Routing Protocol is "bgp 1"
  Cluster Id is set to 10.10.10.0
  Router Id is set to 10.10.10.0
  Fast-external-fallover enabled
Regular expression evaluation optimization enabled
  Capable of ROUTE_REFRESH
  For Address Family IPv4 Unicast
    BGP table version is 0, main routing table version 0
    Distance: external 20 internal 200 local 200
```

bgp router-id

Assign a user-given ID to a BGP router.

S5000

Syntax

```
bgp router-id ip-address
```

To delete a user-assigned IP address, use the `no bgp router-id` command.

Parameters

ip-address	Enter an IP address in dotted decimal format to reset only that BGP neighbor.

Defaults

The router ID is the highest IP address of the Loopback interface or, if no Loopback interfaces are configured, the highest IP address of a physical interface on the router.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Peering sessions are reset when you change the router ID of a BGP router.

bgp soft-reconfig-backup

Use this command *only* when route-refresh is *not* negotiated to avoid the peer from resending messages.

S5000

Syntax

```
bgp soft-reconfig-backup
```

To return to the default setting, use the `no bgp soft-reconfig-backup` command.

Defaults

Off

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you enable soft-reconfiguration for a neighbor and you execute the `clear ip bgp soft in` command, the update database stored in the router is replayed and updates are reevaluated. With this command, the replay and update process is triggered only if route-refresh request is not negotiated with the peer. If the request is indeed negotiated (after executing the `clear ip bgp soft in` command), BGP sends a route-refresh request to the neighbor and receives all of the peer's updates.

NOTE: This command is supported in BGP Router Configuration mode for IPv4 Unicast address only.

Related Commands	clear ip bgp – activates inbound policies without resetting the BGP TCP session.

capture bgp-pdu max-buffer-size

Set the size of the BGP packet capture buffer. This buffer size pertains to both IPv4 and IPv6 addresses.

S5000

Syntax

```
capture bgp-pdu max-buffer-size 100-102400000
```

Parameters

100-102400000	Enter a size for the capture buffer.

Defaults	**40960000 bytes.**
Command Modes	EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands	capture bgp-pdu neighbor – enables capture of an IPv4 BGP neighbor packet. capture bgp-pdu neighbor (ipv6) – enables capture of an IPv6 BGP neighbor packet.

capture bgp-pdu neighbor

Enable capture of an IPv4 BGP neighbor packet.

S5000

Syntax

```
capture bgp-pdu neighbor ipv4-address direction {both | rx |
tx}
```

To disable capture of the IPv4 BGP neighbor packet, use the `no capture bgp-pdu neighbor ipv4-address` command.

Parameters

ipv4-address	Enter the IPv4 address of the target BGP neighbor.
direction {both | rx | tx}	Enter the keyword `direction` and a direction—either `rx` for inbound, `tx` for outbound, or both.

Defaults	Not configured.
Command Modes	EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

capture bgp-pdu max-buffer-size – specifies a size for the capture buffer.

show capture bgp-pdu neighbor – displays BGP packet capture information.

clear ip bgp

Reset BGP sessions on the S5000. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

S5000

Syntax

```
clear ip bgp * | as-number [soft [in | out] | ip-address [soft
[in | out]] | dampening | flap-statistics | ipv4 | ipv6 | peer-
group ]
```

Parameters

*****	Enter an asterisk (*) to reset all BGP sessions.
as-number	Enter the AS number to reset all neighbors belonging to that AS. If used without a qualifier, the keyword resets all neighbors belonging to that AS. The range is 0 to 65535 (2-byte), 1 to 4294967295 (4-byte), or 0.1 to 65535.65535 (dotted format).
ip-address	Enter an IP address in dotted decimal format to reset all prefixes from that neighbor.
dampening	(OPTIONAL) Enter the keyword `dampening` to reset route flap dampening information on that neighbor.
flap-statistics	(OPTIONAL) Enter the keyword `flap-statistics` to reset the flap statistics on all prefixes from that neighbor.
ipv4	(OPTIONAL) Enter the keyword `ipv4` to select options for that address family.
ipv6	(OPTIONAL) Enter the keyword `ipv6` to select options for that address family.
soft	(OPTIONAL) Enter the keyword `soft` to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration. **NOTE:** If you enter the `clear ip bgp ip-address soft` command, both inbound and outbound policies are reset.
in	(OPTIONAL) Enter the keyword `in` to activate only inbound policies.
out	(OPTIONAL) Enter the keyword `out` to activate only outbound policies.
peer-group ***peer-group-name***	(OPTIONAL) Enter the keyword `peer-group` followed by the peer group name to reset the BGP sessions within that peer group.

Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	bgp recursive-bgp-next-hop – disables next-hop resolution through other routes learned by the BGP. bgp soft-reconfig-backup – turns on BGP Soft Reconfiguration.

clear ip bgp dampening

Clear information on route dampening and return the suppressed route to the Active state.

S5000

Syntax

```
clear ip bgp dampening [ip-address mask]
```

Parameters

ip-address mask	(OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) to clear dampening information only for that BGP neighbor.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information After you enter this command, the software deletes the history routes and returns the suppressed routes to the Active state.

clear ip bgp flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

S5000

Syntax

```
clear ip bgp flap-statistics [ip-address mask | filter-list as-
path-name | regexp regular-expression]
```

Parameters

ip-address mask	(OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) to reset only that prefix.
filter-list *as-path-name*	(OPTIONAL) Enter the keywords `filter-list` followed by the name of a configured AS-PATH list.

regexp *regular-expression*	(OPTIONAL) Enter the keyword `regexp` followed by regular expressions. Use one or a combination of the following:

- `.` = (period) any single character (including a white space).
- `*` = (asterisk) the sequences in a pattern (0 or more sequences).
- `+` = (plus) the sequences in a pattern (1 or more sequences).
- `?` = (question mark) sequences in a pattern (either 0 or 1 sequences).

  NOTE: You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression.
- `[ ]` = (brackets) a range of single-character patterns.
- `( )` = (parenthesis) groups a series of pattern elements to a single element.
- `{ }` = (braces) minimum and the maximum match count.
- `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$` = (dollar sign) the end of the output string.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If you enter the `clear ip bgp flap-statistics` command without any parameters, all statistics are cleared.

Related Commands

show debugging – views the enabled debugging operations.

show ip bgp flap-statistics – views the BGP flap statistics.

undebug all – disables all debugging operations.

clear ip bgp peer-group

Reset a peer-group's BGP sessions.

S5000

Syntax `clear ip bgp peer-group peer-group-name`

Parameters

peer-group-name	Enter the peer group name to reset the BGP sessions within that peer group.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug ip bgp

Display all information on BGP, including BGP events, keepalives, notifications, and updates.

S5000

Syntax

```
debug ip bgp [ip-address | peer-group peer-group-name] [in |
out]
```

To disable all BGP debugging, use the `no debug ip bgp` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group ***peer-group-name***	Enter the keywords `peer-group` followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view only information on inbound BGP routes.
out	(OPTIONAL) Enter the keyword `out` to view only information on outbound BGP routes.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To view information on both incoming and outgoing routes, do not include the `in` and `out` parameters in the debugging command. The `in` and `out` parameters cancel each other; for example, if you enter the `debug ip bgp in` command and then enter the `debug ip bgp out` command, you will not see information on the incoming routes.

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

Related Commands

debug ip bgp events – views information about BGP events.

debug ip bgp keepalives – views information about BGP keepalives.

debug ip bgp notifications – views information about BGP notifications.

debug ip bgp updates – views information about BGP updates.

show debugging – views enabled debugging operations.

debug ip bgp dampening

View information on routes being dampened.

S5000

Syntax	`debug ip bgp ipv4 multicast dampening` To disable debugging, use the `no debug ip bgp ipv4 multicast dampening` command.
Parameters	**dampening** — Enter the keyword `dampening` to clear route flap dampening information.
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

debug ip bgp events

Display information on local BGP state changes and other BGP events.

S5000

Syntax

```
debug ip bgp [ip-address | peer-group peer-group-name] events
[in | out]
```

To disable debugging, use the `no debug ip bgp [`*`ip-address`*` | peer-group `*`peer-group-name`*`] events` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword `peer-group` followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view only events on inbound BGP messages.
out	(OPTIONAL) Enter the keyword `out` to view only events on outbound BGP messages.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	Enter the `no debug ip bgp` command to remove all configured debug commands for BGP.

debug ip bgp keepalives

Display information about BGP keepalive messages.

S5000

Syntax

```
debug ip bgp [ip-address | peer-group peer-group-name]
keepalives [in | out]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] keepalives [in | out]` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword `peer-group` followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view only inbound keepalive messages.
out	(OPTIONAL) Enter the keyword `out` to view only outbound keepalive messages.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	Enter the `no debug ip bgp` command to remove all configured debug commands for BGP.

debug ip bgp notifications

Allows you to view information about BGP notifications received from neighbors.

S5000

Syntax

```
debug ip bgp [ip-address | peer-group peer-group-name]
notifications [in | out]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] notifications [in | out]` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword `peer-group` followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view BGP notifications received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view BGP notifications sent to neighbors

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Enter the `no debug ip bgp` command to remove all configured debug commands for BGP.

debug ip bgp peer-group updates

View information about BGP peer-group updates.

S5000

Syntax `debug ip bgp peer-group` *`peer-group-name`* `updates [in | out]`

To disable debugging, use the `no debug ip bgp peer-group` *`peer-group-name`* `updates [in | out]` command.

Parameters

peer-group *peer-group-name*	Enter the keywords `peer-group` followed by the name of the peer-group.
updates	Enter the keyword `updates` to view BGP update information.
in	(OPTIONAL) Enter the keyword `in` to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view only BGP updates sent to neighbors.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug ip bgp soft-reconfiguration

Enable soft-reconfiguration debug.

S5000

Syntax

`debug ip bgp {ip-address | peer-group-name} soft-reconfiguration`

To disable, use the `no debug ip bgp {ip-address | peer-group-name} soft-reconfiguration` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group to disable or enable all routers within the peer group..

Defaults Disabled

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command turns on BGP soft-reconfiguration inbound debugging. If no neighbor is specified, debug turns on for all neighbors.

debug ip bgp updates

Allows you to view information about BGP updates.

S5000

Syntax

`debug ip bgp updates [in | out | prefix-list prefix-list-name]`

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] updates [in | out]` command.

Parameters

in	(OPTIONAL) Enter the keyword `in` to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view only BGP updates sent to neighbors.
prefix-list *prefix-list-name*	(OPTIONAL) Enter the keyword `prefix-list` followed by the name of an established prefix list. If the prefix list is not configured, the default is **permit** (to allow all routes).
ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.

peer-group-name	(OPTIONAL) Enter the name of the peer group to disable or enable all routers within the peer group.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Enter the `no debug ip bgp` command to remove all configured debug commands for BGP.

default-metric

Allows you to change the metric of redistributed routes to locally originated routes. Use this command with the `redistribute` command.

S5000

Syntax `default-metric` *`number`*

To return to the default setting, use the `no default-metric` command.

Parameters

number	Enter a number as the metric to be assigned to routes from other protocols. The range is 1 to 4294967295.

Defaults 0

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The `default-metric` command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.

Related Commands

bgp always-compare-med – enables comparison of all BGP MED attributes.

redistribute – redistributes routes from other routing protocols into BGP.

description

Enter a description of the BGP routing protocol

S5000

Syntax `description {`*`description`*`}`

To remove the description, use the `no description {`*`description`*`}` command.

Parameters

description	Enter a description to identify the BGP protocol (80 characters maximum).

Defaults none

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands router bgp – enters ROUTER mode on the switch.

distance bgp

Define an administrative distance for routes.

S5000

Syntax

`distance bgp` *`external-distance internal-distance local-distance`*

To return to default values, use the `no distance bgp` command.

Parameters

external-distance	Enter a number to assign to routes learned from a neighbor external to the AS. The range is 1 to 255. The default is **20**.
internal-distance	Enter a number to assign to routes learned from a router within the AS. The range is 1 to 255. The default is **200**.
local-distance	Enter a number to assign to routes learned from networks listed in the network command. The range is 1 to 255. The default is **200**.

Defaults

- external-distance = **20**
- internal-distance = **200**
- local-distance = **200**

Command Modes ROUTER BGP (conf-router_bgp_af)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

CAUTION: Dell Networking recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as internal BGP routes.

max-paths

Configure the maximum number of parallel routes (multipath support) BGP supports.

S5000

Syntax `max-paths {ebgp | ibgp} number`

To return to the default values, enter the `no maximum-paths` command.

Parameters

ebgp	Enter the keyword `ebgp` to enable multipath support for External BGP routes.
ibgp	Enter the keyword `ibgp` to enable multipath support for Internal BGP routes.
number	Enter a number as the maximum number of parallel paths. The range is 2 to 64.

Defaults none

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If you enable this command, use the `clear ip bgp *` command to recompute the best path.

neighbor activate

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI (Address Family Identifier/Subsequent Address Family Identifier).

S5000

Syntax `neighbor [ip-address | peer-group-name] activate`

To disable, use the `no neighbor [ip-address | peer-group-name] activate` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group.
activate	Enter the keyword `activate` to enable the neighbor/peer group in the new AFI/SAFI.

Defaults Disabled

Command Modes CONFIGURATION-ROUTER-BGP-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information By default, when you create a neighbor/peer group configuration in the Router BGP context, this enables IPv4/Unicast AFI/SAFI. When you use `activate` in the new context, the neighbor/peer group enables for AFI/SAFI.

neighbor add-path

This command allows the specified neighbor/peer group to send/receive multiple path advertisements.

S5000

Syntax

```
neighbor [ip-address | peer-group-name] add-path [send |
receive | both] count
```

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group.
send	Enter the keyword `send` to indicate that the system will send multiple paths to peers.
receive	Enter the keyword `receive` to indicate that the system will accept multiple paths from peers.
both	Enter the keyword `both` to indicate that the system will send and accept multiple paths from peers.
count	Enter the number paths supported. The range is 2 to 64.

Defaults none

Command Modes CONFIGURATION-ROUTER-BGP-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands bgp add-path – allows the advertisement of multiple paths for the same address prefix without the new paths implicitly replacing any previous ones.

neighbor advertisement-interval

Set the advertisement interval between BGP neighbors or within a BGP peer group.

S5000

Syntax

```
neighbor {ip-address | peer-group-name} advertisement-interval
seconds
```

To return to the default value, use the `no neighbor {ip-address | peer-group-name} advertisement-interval` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
seconds	Enter a number as the time interval, in seconds, between BGP advertisements. The range is 0 to 600 seconds. The default is **5 seconds** for internal BGP peers and **30 seconds** for external BGP peers.

Defaults

- seconds = **5 seconds** (internal peers)
- seconds = **30 seconds** (external peers)

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

neighbor advertisement-start

Set the minimum interval before starting to send BGP routing updates.

S5000

Syntax

```
neighbor {ip-address} advertisement-start seconds
```

To return to the default value, use the `no neighbor {ip-address} advertisement-start` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
seconds	Enter a number as the time interval, in seconds, before BGP route updates are sent. The range is 0 to 3600 seconds.

Defaults	none
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.

neighbor allowas-in

Set the number of times an AS number can occur in the AS path.

S5000

Syntax

`neighbor {`*`ip-address`*` | `*`peer-group-name`*`} allowas-in `*`number`*

To return to the default value, use the `no neighbor {`*`ip-address`*` | `*`peer-group-name`*`} allowas-in` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
number	Enter a number of times to allow this neighbor ID to use the AS path. The range is 1 to 10.

Defaults	Not configured.
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	bgp four-octet-as-support – enables 4-byte support for the BGP process.

neighbor default-originate

Inject the default route to a BGP peer or neighbor.

S5000

Syntax

`neighbor {`*`ip-address`*` | `*`peer-group-name`*`} default-originate [route-map `*`map-name`*`]`

To remove a default route, use the `no neighbor {`*`ip-address`*` | `*`peer-group-name`*`} default-originate` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the default route of all routers in that peer group.
route-map *map-name*	(OPTIONAL) Enter the keyword `route-map` followed by the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If you apply a route map to a BGP peer or neighbor with the `neighbor default-originate` command configured, the software does not apply the set filters in the route map to that BGP peer or neighbor.

neighbor description

Assign a character string describing the neighbor or group of neighbors (peer group).

S5000

Syntax `neighbor {ip-address | peer-group-name} description text`

To delete a description, use the `no neighbor {ip-address | peer-group-name} description` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
text	Enter a continuous text string up to 80 characters.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

neighbor distribute-list

Distribute BGP information via an established prefix list.

S5000

Syntax

`neighbor {ip-address | peer-group-name} distribute-list prefix-list-name {in | out}`

To delete a neighbor distribution list, use the `no neighbor {ip-address | peer-group-name} distribute-list prefix-list-name {in | out}` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to apply the distribute list filter to all routers in the peer group.
prefix-list-name	Enter the name of an established prefix list. If the prefix list is not configured, the default is **permit** (to allow all routes).
in	Enter the keyword `in` to distribute only inbound traffic.
out	Enter the keyword `out` to distribute only outbound traffic.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Other BGP filtering commands include: `neighbor filter-list`, `ip as-path access-list`, and `neighbor route-map`.

Related Commands

ip as-path access-list – configures IP AS-Path ACL.

neighbor filter-list – assigns a AS-PATH list to a neighbor or peer group.

neighbor route-map – assigns a route map to a neighbor or peer group.

neighbor ebgp-multihop

Attempt and accept BGP connections to external peers on networks that are not directly connected.

S5000

Syntax

`neighbor {ip-address | peer-group-name} ebgp-multihop [ttl]`

To disallow and disconnect connections, use the `no neighbor {ip-address | peer-group-name} ebgp-multihop` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
ttl	(OPTIONAL) Enter the number of hops as the Time to Live (ttl) value. The range is 1 to 255. The default is **255**.

Defaults Disabled.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information To prevent loops, the `neighbor ebgp-multihop` command does not install the default routes of the multihop peer. Networks not directly connected are not considered valid for best-path selection.

neighbor fail-over

Enable or disable fast fail-over for BGP neighbors.

S5000

Syntax `neighbor {ipv4-address | peer-group-name} fall-over`

To disable, use the `no neighbor {ipv4-address | peer-group-name} fall-over` command.

Parameters

ipv4-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.

Defaults Disabled.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information When you enable fail-over, BGP keeps track of IP or IPv6 ability to reach the peer remote address and the peer local address. Whenever either address becomes unreachable (for example, no active route exists in the routing table for the peer IP or IPv6 destination/local address), BGP brings down the session with the peer.

Related Commands show ip bgp neighbors – displays information on the BGP neighbors.

neighbor filter-list

Configure a BGP filter based on the AS-PATH attribute.

S5000

Syntax

`neighbor {`*`ip-address`*` | `*`peer-group-name`*`} filter-list `*`as-path-name`*` {in | out}`

To delete a BGP filter, use the `no neighbor {`*`ip-address`*` | `*`peer-group-name`*`} filter-list `*`as-path-name`*` {in | out}` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to apply the filter to all routers in the peer group.
as-path-name	Enter the name of an established AS-PATH access list (up to 140 characters). If the AS-PATH access list is not configured, the default is **permit** (allow routes).
in	Enter the keyword `in` to filter inbound BGP routes.
out	Enter the keyword `out` to filter outbound BGP routes.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `ip as-path access-list` command in CONFIGURATION mode to enter AS-PATH ACL mode and configure the AS-PATH filters to deny or permit BGP routes based on information in their AS-PATH attribute.

Related Commands

ip as-path access-list – enter AS-PATH ACL mode and configure the AS-PATH filters.

neighbor graceful-restart

Enable graceful restart on a BGP neighbor.

S5000

Syntax

`neighbor {`*`ip-address`*` | `*`peer-group-name`*`} graceful-restart [restart-time `*`seconds`*`] [stale-path-time `*`seconds`*`] [role receiver-only]`

To return to the default, enter the `no bgp graceful-restart` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to apply the filter to all routers in the peer group.
restart-time *seconds*	Enter the keyword `restart-time` followed by the maximum number of seconds needed to restart and bring-up all the peers. The range is 1 to 3600 seconds. The default is **120 seconds**.
stale-path-time *seconds*	Enter the keyword `stale-path-time` followed by the maximum number of seconds to wait before restarting a peer's stale paths. The default is **360 seconds**.
role receiver-only	Enter the keyword `role receiver-only` to designate the local router to support graceful restart as a receiver only.

Defaults as above

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This feature advertises to BGP neighbors through a capability advertisement. In Receiver Only mode, BGP saves the advertised routes of peers that support this capability when they restart.

neighbor local-as

Configure Internal BGP (IBGP) routers to accept external routes from neighbors with a local AS number in the AS number path.

S5000

Syntax `neighbor {ip-address | peer-group-name} local-as as-number [no-prepend]`

To return to the default value, use the `no neighbor {ip-address | peer-group-name} local-as` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
as-number	Enter the AS number to reset all neighbors belonging to that AS. The range is 0 to 65535 (2-byte), 1 to 4294967295 (4-byte) or 0.1 to 65535.65535 (dotted format).
no prepend	Specifies that local AS values do not prepend to announcements from the neighbor.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

bgp four-octet-as-support – enables 4-byte support for the BGP process.

neighbor maximum-prefix

Control the number of network prefixes received.

S5000

Syntax

```
neighbor {ip-address | peer-group-name} maximum-prefix maximum
[threshold] [warning-only]
```

To return to the default values, use the `no neighbor {ip-address | peer-group-name} maximum-prefix maximum` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
maximum	Enter a number as the maximum number of prefixes allowed for this BGP router. The range is 1 to 4294967295.
threshold	(OPTIONAL) Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches this threshold, the switch software sends a message. The range is 1 to 100 percent. The default is **75**.
warning-only	(OPTIONAL) Enter the keyword `warning-only` to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

Defaults

threshold = **75**

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you configure the `neighbor maximum-prefix` command and the neighbor receives more prefixes than allowed by the `neighbor maximum-prefix` command configuration, the neighbor goes down and the `show ip bgp summary` command displays (prfxd) in the State/PfxRcd column for that neighbor. The neighbor remains down until you enter the `clear ip bgp` command for the neighbor or the peer group to which the neighbor belongs or you enter the `neighbor shutdown` and `neighbor no shutdown` commands.

Related Commands show ip bgp summary – displays the current BGP configuration.

neighbor next-hop-self

Allows you to configure the router as the next hop for a BGP neighbor. (This command is used for IBGP).

S5000

Syntax

`neighbor {ip-address | peer-group-name} next-hop-self`

To return to the default setting, use the `no neighbor {ip-address | peer-group-name} next-hop-self` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.

Defaults Disabled.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If you configure the `set next-hop` command in ROUTE-MAP mode, the configuration takes precedence over the `neighbor next-hop-self` command.

neighbor password

Enable message digest 5 (MD5) authentication on the TCP connection between two neighbors.

S5000

Syntax

`neighbor {ip-address | peer-group-name} password [encryption-type] password`

To delete a password, use the `no neighbor {ip-address | peer-group-name} password` command.

Parameters

ip-address	Enter the IP address of the router to be included in the peer group.
peer-group-name	Enter the name of a configured peer group.
encryption-type	(OPTIONAL) Enter `7` as the encryption type for the password entered. `7` means that the password is encrypted and hidden.
password	Enter a text string up to 80 characters long. The first character of the password must be a letter.

You cannot use spaces in the password.

Defaults	Not configured.
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Usage Information

Configure the same password on both BGP peers or a connection does not occur. When you configure MD5 authentication between two BGP peers, each segment of the TCP connection between them is verified and the MD5 digest is checked on every segment sent on the TCP connection.

Configuring a password for a neighbor causes an existing session to be torn down and a new one established.

If you specify a BGP peer group by using the `peer-group-name` parameter, all the members of the peer group inherits the characteristic configured with this command.

If you configure a password on one neighbor, but you have not configured a password for the neighboring router, the following message appears on the console while the routers attempt to establish a BGP session between them:

```
%STKUNIT0-M:CP %KERN-6-INT: No BGP MD5 from [peer's IP address]
:179 to [local router's IP address]:65524
```

Also, if you configure different passwords on the two routers, the following message appears on the console:

```
%STKUNIT0-M:CP %KERN-6-INT: BGP MD5 password mismatch from
[peer's IP address] : 11502 to [local router's IP address] :179
```

neighbor peer-group (assigning peers)

Allows you to assign one peer to a existing peer group.

S5000

Syntax

`neighbor ip-address peer-group peer-group-name`

To delete a peer from a peer group, use the `no neighbor ip-address peer-group peer-group-name` command.

Parameters

ip-address	Enter the IP address of the router to be included in the peer group.
peer-group-name	Enter the name of a configured peer group.

Defaults	Not configured.
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Usage Information

You can assign up to 256 peers to one peer group.

When you add a peer to a peer group, it inherits all the peer group's configured parameters. A peer cannot become part of a peer group if any of the following commands are configured on the peer:

- neighbor advertisement-interval
- neighbor distribute-list
- neighbor filter-list
- neighbor next-hop-self
- neighbor route-map
- neighbor route-reflector-client
- neighbor send-community

A neighbor may keep its configuration after it was added to a peer group if the neighbor's configuration is more specific than the peer group's, and the neighbor's configuration does not affect outgoing updates.

A peer group must exist before you add a peer to it. If the peer group is disabled (shutdown) the peers within the group are also disabled (shutdown).

Related Commands

clear ip bgp – resets BGP sessions.

neighbor peer-group (creating group) – creates a peer group.

show ip bgp peer-group – views BGP peers.

show ip bgp neighbors – views BGP neighbors configurations.

neighbor peer-group (creating group)

Allows you to create a peer group and assign it a name.

S5000

Syntax

`neighbor` *`peer-group-name`* `peer-group`

To delete a peer group, use the `no neighbor` *`peer-group-name`* `peer-group` command.

Parameters

peer-group-name	Enter a text string up to 16 characters long as the name of the peer group.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	When you create a peer group, it is disabled (Shut mode).
Related Commands	neighbor peer-group (assigning peers) – assigns routers to a peer group. neighbor remote-as – assigns a indirectly connected AS to a neighbor or peer group. neighbor shutdown – disables a peer or peer group.

neighbor peer-group passive

Enable passive peering on a BGP peer group, that is, the peer group does not send an OPEN message, but will respond to one.

S5000

Syntax

`neighbor` *`peer-group-name`* `peer-group passive [limit` *`sessions`*`]`

To delete a passive peer-group, use the `no neighbor` *`peer-group-name`* `peer-group passive` command.

Parameters

peer-group-name	Enter a text string up to 16 characters long as the name of the peer group.
limit	Enter the keyword `limit` to constrain the numbers of sessions for this peer-group. The range is 2 to 256. The default is **256**.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

After you configure a peer group as passive, you must assign it a subnet using the `neighbor soft-reconfiguration inbound` command.

For passive eBGP limits, the Remote AS must be different from the AS for this neighbor.

Related Commands

neighbor soft-reconfiguration inbound– assigns a subnet to a dynamically-configured BGP neighbor.

neighbor remote-as – assigns an indirectly connected AS to a neighbor or peer group.

neighbor remote-as

Create and specify the remote peer to the BGP neighbor.

S5000

Syntax	`neighbor {`*`ip-address`*`	`*`peer-group-name`*`} remote-as `*`number`* To delete a remote AS entry, use the `no neighbor {`*`ip-address`*`	`*`peer-group-name`*`} remote-as `*`number`* command.
Parameters	

ip-address	Enter the IP address of the neighbor to enter the remote AS in its routing table.
peer-group-name	Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.
number	Enter a number of the AS. The range is 0 to 65535 (2-byte) or 1 to 4294967295 (4-byte).

Defaults	Not configured.
Command Modes	ROUTER BGP
Command History	

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must configure your system to accept 4-byte formats before entering a 4-byte AS Number. If the `number` parameter is the same as the AS number used in the `router bgp` command, the remote AS entry in the neighbor is considered an internal BGP peer entry.

This command creates a peer and the newly created peer is disabled (Shutdown).

Related Commands

router bgp – enters ROUTER BGP mode and configures routes in an AS.

bgp four-octet-as-support – enables 4-byte support for the BGP process.

neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

S5000

Syntax	`neighbor {`*`ip-address`*`	`*`peer-group-name`*`} remove-private-as` To return to the default, use the `no neighbor {`*`ip-address`*`	`*`peer-group-name`*`} remove-private-as` command.
Parameters	

ip-address	Enter the IP address of the neighbor to remove the private AS numbers.

peer-group-name	Enter the name of the peer group to remove the private AS numbers.

Defaults Disabled (that is, private AS number are not removed).

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Applies to EBGP neighbors only.

You must configure your system to accept 4-byte formats before entering a 4-byte AS Number.

If the AS-PATH contains both public and private AS number or contains AS numbers of an EBGP neighbor, the private AS numbers are not removed.

If a confederation contains private AS numbers in its AS-PATH, the software removes the private AS numbers only if they follow the confederation numbers in the AS path.

Private AS numbers are 64512 to 65535 (2-byte).

neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

S5000

Syntax

```
neighbor {ip-address | peer-group-name} route-map map-name {in
| out}
```

To remove the route map, use the `no neighbor {ip-address | peer-group-name} route-map map-name {in | out}` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
map-name	Enter the name of an established route map. If the Route map is not configured, the default is **deny** (to drop all routes).
in	Enter the keyword `in` to filter inbound routes.
out	Enter the keyword `out` to filter outbound routes.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

Configure the router as a route reflector and the specified neighbors as members of the cluster.

S5000

Syntax

`neighbor {ip-address | peer-group-name} route-reflector-client`

To remove one or more neighbors from a cluster, use the `no neighbor {ip-address | peer-group-name} route-reflector-client` command. If you delete all members of a cluster, you also delete the route-reflector configuration on the router.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

A route reflector reflects routes to the neighbors assigned to the cluster. Neighbors in the cluster do not need not be fully meshed. By default, when you use `no route reflector`, the internal BGP (IBGP) speakers in the network must be fully meshed.

The first time you enter this command, the router configures as a route reflector and the specified BGP neighbors configure as clients in the route-reflector cluster.

When you remove all clients of a route reflector using the `no neighbor route-reflector-client` command, the router no longer functions as a route reflector.

If the clients of a route reflector are fully meshed, you can configure the route reflector to not reflect routes to specified clients by using the `no bgp client-to-client reflection` command.

Related Commands

bgp client-to-client reflection – enables route reflection between the route reflector and the clients.

neighbor send-community

Send a COMMUNITY attribute to a BGP neighbor or peer group. A COMMUNITY attribute indicates that all routes with that attribute belong to the same community grouping.

S5000

Syntax

`neighbor {ip-address | peer-group-name} send-community`

To disable sending a COMMUNITY attribute, use the `no neighbor {ip-address | peer-group-name} send-community` command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to send a COMMUNITY attribute to all routers within the peer group.

Defaults Not configured and COMMUNITY attributes are not sent to neighbors.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information To configure a COMMUNITY attribute, use the `set community` command in ROUTE-MAP mode.

neighbor shutdown

Disable a BGP neighbor or peer group.

S5000

Syntax

`neighbor {ip-address | peer-group-name} shutdown`

To enable a disabled neighbor or peer group, use the `neighbor {ip-address | peer-group-name} no shutdown` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults Enabled (that is, BGP neighbors and peer groups are disabled.)

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	Peers that are enabled within a peer group are disabled when their peer group is disabled. The `neighbor shutdown` command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the specified BGP sessions. When a neighbor or peer group is shutdown, use the `show ip bgp summary` command to confirm its status.
Related Commands	show ip bgp summary – displays the current BGP configuration. show ip bgp neighbors – displays the current BGP neighbors.

neighbor soft-reconfiguration inbound

Enable soft-reconfiguration for BGP.

S5000

Syntax

```
neighbor {ip-address | peer-group-name} soft-reconfiguration
inbound
```

To disable, use the `no neighbor {ip-address | peer-group-name} soft-reconfiguration inbound` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults Disabled

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command enables soft-reconfiguration for the BGP neighbor specified. BGP stores all the updates received by the neighbor but does not reset the peer-session.

CAUTION: Inbound update storage is a memory-intensive operation. The entire BGP update database from the neighbor is stored in memory regardless of the inbound policy results applied on the neighbor.

NOTE: This command is supported in BGP Router Configuration mode for IPv4 Unicast address only.

Related Commands

show ip bgp neighbors – displays routes received by a neighbor.

neighbor subnet

Enable passive peering so that the members of the peer group are dynamic.

S5000

Syntax

`neighbor peer-group-name subnet subnet-number mask`

To remove passive peering, use the `no neighbor peer-group-name subnet subnet-number mask` command.

Parameters

subnet-number	Enter a subnet number in dotted decimal format (A.B.C.D.) as the allowable range of addresses included in the Peer group. To allow all addresses, enter `0.0.0.0/0`.
mask	Enter a prefix mask in / prefix-length format (/x).

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

neighbor timers

Set keepalive and hold time timers for a BGP neighbor or a peer group.

S5000

Syntax

`neighbor {ip-address | peer-group-name} timers keepalive holdtime`

To return to the default values, use the `no neighbor {ip-address | peer-group-name} timers` command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the timers for all routers within the peer group.
keepalive	Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. The range is 1 to 65535. The default is **60 seconds**.
holdtime	Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. The range is 3 to 65535. The default is **180 seconds**.

Defaults	- keepalive = **60 seconds** - holdtime = **180 seconds**
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Timer values configured with the `neighbor timers` command overrides the timer values configured with the any other command. When two neighbors, configured with different `keepalive` and `holdtime` values, negotiate for new values, the resulting values are as follows: - the lower of the `holdtime` values is the new `holdtime` value, and - whichever is the lower value; one-third of the new `holdtime` value, or the configured `keepalive` value, is the new keepalive value.

neighbor update-source

Enable the S5000 software to use Loopback interfaces for TCP connections for BGP sessions.

S5000

Syntax

`neighbor {`*`ip-address`*` | `*`peer-group-name`*`} update-source `*`interface`*

To use the closest interface, use the `no neighbor {`*`ip-address`*` | `*`peer-group-name`*`} update-source `*`interface`* command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to disable all routers within the peer group.
interface	Enter the keyword `loopback` followed by a number of the Loopback interface. The range is 0 to 16383.

Defaults	Not configured.
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The `neighbor update-source` command is not necessary for directly connected internal BGP sessions.

neighbor weight

Assign a weight to the neighbor connection, which is used to determine the best path.

S5000

Syntax

`neighbor {ip-address | peer-group-name} weight weight`

To remove a weight value, use the `no neighbor {ip-address | peer-group-name} weight` command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to disable all routers within the peer group.
weight	Enter a number as the weight. The range is 0 to 65535. The default is **0**.

Defaults

0

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

In the FTOS best path selection process, the path with the highest weight value is preferred.

> **NOTE:** In the FTOS best-path selection process, the path with the highest weight value is preferred.

If you configure the `set weight` command in a route map applied to this neighbor, the weight set in that command overrides the weight set in the `neighbor weight` command.

Related Commands

set weight – assigns a weight to all paths meeting the route map criteria.

network

Specify the networks for the BGP process and enter them in the BGP routing table.

S5000

Syntax

`network ip-address mask [route-map map-name]`

To remove a network, use the `no network ip-address mask [route-map map-name]` command.

Parameters

ip-address	Enter an IP address in dotted decimal format of the network.
mask	Enter the mask of the IP address in the slash prefix length format (for example, /24).

	The mask appears in command outputs in dotted decimal format (A.B.C.D).
route-map *map-name*	(OPTIONAL) Enter the keyword `route-map` followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ip address • set community • set local-preference • set metric • set next-hop • set origin • set weight If the route map is not configured, the default is **deny** (to drop all routes).

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information FTOS software resolves the network address configured by the `network` command with the routes in the main routing table to ensure that the networks are reachable using non-BGP routes and non-default routes.

Related Commands redistribute – redistributes routes into BGP.

network backdoor

Specify this IGP route as the preferred route.

S5000

Syntax

`network ip-address mask backdoor`

To remove a network, use the `no network ip-address mask backdoor` command.

Parameters

ip-address	Enter an IP address in dotted decimal format of the network.
mask	Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).

Defaults	Not configured.
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Although FTOS does not generate a route due to the backdoor config, there is an option for injecting/sourcing a local route in the presence of network backdoor config on a learned route.

redistribute

Redistribute routes into BGP.

S5000

Syntax

`redistribute {connected | static} [route-map map-name]`

To disable redistribution, use the `no redistribution {connected | static}` command.

Parameters

connected	Enter the keyword `connected` to redistribute routes from physically connected interfaces.
static	Enter the keyword `static` to redistribute manually configured routes. These routes are treated as incomplete routes.
route-map *map-name*	(OPTIONAL) Enter the keyword `route-map` followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ip address • set community • set local-preference • set metric • set next-hop • set origin • set weight If the route map is not configured, the default is **deny** (to drop all routes).

Defaults	Not configured.
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Usage Information

With FTOS version 8.3.1.0 and later, you can use the `redistribute` command to advertise the IGP cost as the MED on redistributed routes. When you set the route-map with metric-type internal and applied outbound to an EBGP peer/peer-group, the advertised routes corresponding to those peer/peer-group have the IGP cost set as **MED**.

If you do not configure the `default-metric` command, in addition to the `redistribute` command, or there is no route map to set the metric, the metric for redistributed static and connected is "0".

To redistribute the default route (0.0.0.0/0), configure the `neighbor default-originate` command.

Related Commands

neighbor default-originate – injects the default route.

router bgp

Enter ROUTER BGP mode to configure and enable BGP.

S5000

Syntax

`router bgp as-number`

To disable BGP, use the `no router bgp as-number` command.

Parameters

as-number	Enter the AS number. The range is 1 to 65535 (2-byte), 1 to 4294967295 (4-byte), or 0.1 to 65535.65535 (dotted format).

Defaults

Not enabled.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

At least one interface must be in Layer 3 mode for the `router bgp` command to be accepted. If no interfaces are enabled for Layer 3, an error message appears:

```
% Error: No router id
configured
```

Example

```
FTOS(conf)#router bgp 3
FTOS(conf-router_bgp)#
```

show capture bgp-pdu neighbor

Display BGP packet capture information for an IPv4 address on the system.

S5000

Syntax `show capture bgp-pdu neighbor` *`ipv4-address`*

Parameters

ipv4-address	Enter the IPv4 address (in dotted decimal format) of the BGP address to display packet information for that address.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-router_bgp)#show capture bgp-pdu neighbor 20.20.20.2

Incoming packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 40958758, 26 packet(s) captured using
680 bytes
  PDU[1] : len 101, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00650100 00000013
00000000
00000000 419ef06c 00000000
    00000000 00000000 00000000 00000000 0181a1e4 0181a25c
41af92c0
00000000 00000000 00000000
    00000000 00000001 0181a1e4 0181a25c 41af9400 00000000
  PDU[2] : len 19, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
  PDU[3] : len 19, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
 [. . .]

Outgoing packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 40958758, 27 packet(s) captured using
562 bytes
  PDU[1] : len 41, captured 00:34:52 ago
    ffffffff ffffffff ffffffff ffffffff 00290104 000100b4
14141401
0c020a01 04000100 01020080
    00000000
  PDU[2] : len 19, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
  PDU[3] : len 19, captured 00:34:50 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
 [. . .]
FTOS#
```

Related Commands capture bgp-pdu max-buffer-size – specifies a size for the capture buffer.

show config

View the current ROUTER BGP configuration.

S5000

Syntax	`show config`
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
FTOS(conf-router_bgp)#show config
!
router bgp 45
 neighbor suzanne peer-group
 neighbor suzanne no shutdown
 neighbor sara peer-group
 neighbor sara shutdown
 neighbor 13.14.15.20 peer-group suzanne
 neighbor 13.14.15.20 shutdown
 neighbor 123.34.55.123 peer-group suzanne
 neighbor 123.34.55.123 shutdown
FTOS(conf-router_bgp)#
```

Related Commands capture bgp-pdu max-buffer-size – specifies a size for the capture buffer.

show ip bgp

View the current BGP IPv4 routing table for the system.

S5000

Syntax `show ip bgp [ipv4 unicast] [network [network-mask] [longer-prefixes]]`

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
network	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
network-mask	(OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.
longer-prefixes	(OPTIONAL) Enter the keywords `longer-prefixes` to view all routes with a common prefix.

Command Modes

- EXEC

- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you enable the `bgp non-deterministic-med` command, the `show ip bgp` command output for a BGP route does not list the INACTIVE reason.

The following describes the `show ip bgp` command shown in the Example below.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
FTOS>show ip bgp
BGP table version is 847562, local router ID is 63.114.8.131
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network         Next Hop   Metric LocPrf Weight Path
*>  0.0.0.0/0      63.114.8.33                  0 18508 i
*   3.0.0.0/8      63.114.8.33                  0 18508 209
701 80 i
*>                 63.114.8.33                  0 18508 701 80
i
*>  3.3.0.0/16     0.0.0.0        22        32768 ?
                   63.114.8.33                  0 18508 ?
*>  4.0.0.0/8      63.114.8.33                  0 18508 701 1 i
*>  4.2.49.12/30   63.114.8.33                  0 18508 209 i
*   4.17.250.0/24  63.114.8.33                  0 18508 209
1239 13716 i
*>  63.114.8.33                                 0 18508 701
1239 13716 i
*   4.21.132.0/23  63.114.8.33                  0 18508 209
6461 16422 i
*>                 63.114.8.33                  0 18508 701
6461 16422 i
*>  4.24.118.16/30 63.114.8.33                  0 18508 209 i
*>  4.24.145.0/30  63.114.8.33                  0 18508 209 i
*>  4.24.187.12/30 63.114.8.33                  0 18508 209 i
*>  4.24.202.0/30  63.114.8.33                  0 18508 209 i
*>  4.25.88.0/30   63.114.8.33                  0 18508 209
3561 3908 i
*>  5.0.0.0/9      63.114.8.33     0            0 18508 ?
*>  5.0.0.0/10     63.114.8.33     0            0 18508 ?
*>  5.0.0.0/11     63.114.8.33     0            0 18508 ?
--More--
```

Related Commands

show ip bgp community – views the BGP communities.

neighbor maximum-prefix – controls the number of network prefixes received.

show ip bgp cluster-list

View BGP neighbors in a specific cluster.

S5000

Syntax

`show ip bgp [ipv4 unicast] cluster-list [cluster-id]`

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
cluster-id	(OPTIONAL) Enter the cluster id in dotted decimal format.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp cluster-list` command shown in the Example below.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
FTOS#show ip bgp cluster-list
BGP table version is 64444683, local router ID is 120.1.1.1
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n
- network
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop      Metric LocPrf Weight Path
```

```
* I 10.10.10.1/32     192.68.16.1        0    100       0 i
* I                   192.68.16.1        0    100       0 i
*>I                   192.68.16.1        0    100       0 i
* I                   192.68.16.1        0    100       0 i
* I                   192.68.16.1        0    100       0 i
* I                   192.68.16.1        0    100       0 i
* I 10.19.75.5/32     192.68.16.1        0    100       0 ?
* I                   192.68.16.1        0    100       0 ?
*>I                   192.68.16.1        0    100       0 ?
* I                   192.68.16.1        0    100       0 ?
* I                   192.68.16.1        0    100       0 ?
* I                   192.68.16.1        0    100       0 ?
* I 10.30.1.0/24      192.68.16.1        0    100       0 ?
* I                   192.68.16.1        0    100       0 ?
*>I                   192.68.16.1        0    100       0 ?
* I                   192.68.16.1        0    100       0 ?
* I                   192.68.16.1        0    100       0 ?
* I                   192.68.16.1        0    100       0 ?
```

show ip bgp community

View information on all routes with Community attributes or view specific BGP community groups.

S5000

Syntax

`show ip bgp [`*`ipv4 unicast`*`] community [`*`community-number`*`] [local-as] [no-export] [no-advertise]`

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.
local-AS	Enter the keywords `local-AS` to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords `no-advertise` to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords `no-export` to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp` command output.

The following describes the `show ip bgp community` command shown in the Example below.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
FTOS>show ip bgp community
BGP table version is 3762622, local router ID is 63.114.8.48
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

Network            Next Hop   Metric LocPrf Weight Path
* i 3.0.0.0/8      205.171.0.16         100    0 209 701 80 i
*>i 4.2.49.12/30   205.171.0.16         100    0 209 i
* i 4.21.132.0/23  205.171.0.16         100    0 209 6461
16422 i
*>i 4.24.118.16/3  205.171.0.16         100    0 209 i
*>i 4.24.145.0/30  205.171.0.16         100    0 209 i
*>i 4.24.187.12/30 205.171.0.16         100    0 209 i
*>i 4.24.202.0/30  205.171.0.16         100    0 209 i
*>i 4.25.88.0/30   205.171.0.16         100    0 209 3561 3908
i
*>i 6.1.0.0/16     205.171.0.16         100    0 209 7170 1455
i
*>i 6.2.0.0/22     205.171.0.16         100    0 209 7170 1455
i
*>i 6.3.0.0/18     205.171.0.16         100    0 209 7170 1455
i
*>i 6.4.0.0/16     205.171.0.16         100    0 209 7170 1455
i
```

```
*>i 6.5.0.0/19     205.171.0.16         100    0 209 7170 1455
i
*>i 6.8.0.0/20     205.171.0.16         100    0 209 7170 1455
i
*>i 6.9.0.0/20     205.171.0.16         100    0 209 7170 1455
i
*>i 6.10.0.0/15    205.171.0.16         100    0 209 7170 1455
i
*>i 6.14.0.0/15    205.171.0.16         100    0 209 7170 1455
i
*>i 6.133.0.0/21   205.171.0.16         100    0 209 7170 1455
i
*>i 6.151.0.0/1    205.171.0.16         100    0 209 7170 1455
i
--More--
```

show ip bgp community-list

View routes that are affected by a specific community list.

S5000

Syntax

```
show ip bgp [ipv4 unicast] community-list community-list-name
[exact-match]
```

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
community-list-name	Enter the name of a configured IP community list (max 16 characters).
exact-match	Enter the keyword for an exact match of the communities.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `show ip bgp community-list` command without any parameters lists BGP routes matching the Community List and the output is the same as for the `show ip bgp` command output.

The following describes the `show ip bgp community-list pass` command shown in the Example below.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.

Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
FTOS#show ip bgp community-list pass
BGP table version is 0, local router ID is 10.101.15.13
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

Network     Next Hop      Metric     LocPrf     Weight Path
FTOS#
```

show ip bgp dampened-paths

View BGP routes that are dampened (non-active).

S5000

Syntax `show ip bgp [ipv4 unicast] dampened-paths`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp damp` command shown in the Example below.

Field	**Description**
Network	Displays the network ID to which the route is dampened.
From	Displays the IP address of the neighbor advertising the dampened route.
Reuse	Displays the hour:minutes:seconds until the dampened route is available.
Path	Lists all the ASs the dampened route passed through to reach the destination network.

Example

```
FTOS>show ip bgp damp
BGP table version is 210708, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, >
```

```
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network      From       Reuse       Path
FTOS>
```

show ip bgp detail

Display BGP internal information for the IPv4 Unicast address family.

S5000

Syntax `show ip bgp [`*`ipv4 unicast`*`] detail`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip bgp detail
Detail information for BGP Node
bgpNdP 0x41a17000 : NdTmrP 0x41a17000 : NdKATmrP 0x41a17014 :
NdTics 74857 :
NhLocAS 1 : NdState 2 : NdRPMPrim 1 : NdListSoc 13
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfedId 0 : NdMedConfed 0 :
NdMedMissVal -1 :
NdIgnrIllId 0 : NdRRC2C 1 : NdClstId 33686273 : NdPaTblP
0x41a19088
NdASPTblP 0x41a19090 : NdCommTblP 0x41a19098 : NhOptTransTblP
0x41a190a0 :
NdRRClsTblP 0x41a190a8
NdPktPA 0 : NdLocCBP 0x41a6f000 : NdTmpPAP 0x419efc80 :
NdTmpASPAP 0x41a25000 :
NdTmpCommP 0x41a25800
NdTmpRRClP 0x41a4b000 : NdTmpOptP 0x41a4b800 : NdTmpNHP :
NdOrigPAP 0
NdOrgNHP 0 : NdModPathP 0x419efcc0 : NdModASPAP 0x41a4c000 :
NdModCommP 0x41a4c800
NdModOptP 0x41a4d000 : NdModNHP : NdComSortBufP 0x41a19110 :
NdComSortHdP
0x41a19d04 : NdUpdAFMsk 0 : AFRstSet 0x41a1a298 : NHopDfrdHdP
0x41a1a3e0 :

NumNhDfrd 0 : CfgHdrAFMsk 1
AFChkNetTmrP 0x41ee705c : AFRtDamp 0 : AlwysCmpMed 0 : LocrHld
10 : LocrRem 10 :
softReconfig 0x41a1a58c
DefMet 0 : AutoSumm 1 : NhopsP 0x41a0d100 : Starts 0 : Stops
0 : Opens 0
Closes 0 : Fails 0 : Fatals 0 : ConnExps 0 : HldExps 0 :
```

```
KeepExps 0
RxOpens 0 : RxKeeps 0 : RxUpds 0 : RxNotifs 0 : TxUpds 0 :
TxNotifs 0
BadEvts 0 : SynFails 0 : RxeCodeP 0x41a1b6b8 : RxHdrCodeP
0x41a1b6d4 : RxOpCodeP
0x41a1b6e4
RxUpdCodeP 0x41a1b704 : TxEcodeP 0x41a1b734 : TxHdrcodeP
0x41a1b750 : TxOpCodeP
0x41a1b760
TxUpdCodeP 0x41a1b780 : TrEvt 0 : LocPref 100 : tmpPathP
0x41a1b7b8 : LogNbrChgs 1
RecursiveNH 1 : PgCfgId 0 : KeepAlive 0 : HldTime 0 : DioHdl
0 : AggrValTmrP
0x41ee7024
UpdNetTmrP 0 : RedistTmrP 0x41ee7094 : PeerChgTmrP 0 :
CleanRibTmrP 0x41ee7104
PeerUpdTmrP 0x41ee70cc : DfrdNHTmrP 0x41ee7174 : DfrdRtselTmrP
0x41ee713c :
FastExtFailover 1 : FastIntFailover 0 : Enforce1stAS 1
PeerIdBitsP 0x41967120 : softOutSz 16 : RibUpdCtxCBP 0
UpdPeerCtxCBP 0 : UpdPeerCtxAFI 0 : TcpioCtxCB 0 : RedistBlk 1
NextCBPurg 1101119536 : NumPeerToPurge 0 : PeerIBGPCnt 0 :
NonDet 0 : DfrdPathSel 0
BGPRst 0 : NumGrCfg 1 : DfrdTmestmp 0 : SnmpTrps 0 :
IgnrBestPthASP 0
RstOn 1 : RstMod 1 : RstRole 2 : AFFalgs 7 : RstInt 120 :
MaxeorExtInt 361
FixedPartCrt 1 : VarParCrt 1
Packet Capture max allowed length 40960000 : current length 0

Peer Grp List
Nbr List
Confed Peer List
Address Family specific Information
AFIndex 0
NdSpFlag 0x41a190b0 : AFRttP 0x41a0d200 : NdRTMMkrP
0x41a19d28 : NdRTMAFTblVer 0 :
NdRibCtxAddr 1101110688
NdRibCtxAddrLen 255 : NdAFPrefix 0 : NdAfNLRIP 0 : NdAFNLRILen
0 : NdAFWPtrP 0
NdAFWLen 0 : NdAfNH : NdAFRedRttP 0x41a0d400 : NdRecCtxAdd
1101110868
NdRedCtxAddrLen 255 : NdAfRedMkrP 0x41a19e88 : AFAggRttP
0x41a0d600 : AfAggCtxAddr
1101111028 : AfAggrCtxAddrLen 255
AfNumAggrPfx 0 : AfNumAggrASSet 0 : AfNumSuppmap 0 :
AfNumAggrValidPfx 0 :
AfMPathRttP 0x41a0d700
MpathCtxAddr 1101111140 : MpathCtxAddrlen 255 : AfEorSet
0x41a19f98 : NumDfrdPfx 0
AfActPeerHd 0x41a1a3a4 : AfExtDist 1101112312 : AfIntDist
200 : AfLocDist 200
AfNumRRc 0 : AfRR 0 : AfNetRttP 0x41a0d300 : AfNetCtxAddr
1101112392 :
AfNetCtxAddrlen 255
AfNwCtxAddr 1101112443 : AfNwCtxAddrlen 255 : AfNetBKDrRttP
0x41a0d500 :
AfNetBKDRCnt 0 : AfDampHLife 0
AfDampReuse 0 : AfDampSupp 0 : AfDampMaxHld 0 : AfDampCeiling
0 : AfDampRmapP
```

show ip bgp extcommunity-list

View information on all routes with Extended Community attributes.

S5000

Syntax

```
show ip bgp [ipv4 unicast] extcommunity-list [list name]
```

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
list name	Enter the extended community list name you wish to view.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp` command output.

show ip bgp filter-list

View the routes that match the filter lists.

S5000

Syntax

```
show ip bgp [ipv4 unicast] filter-list as-path-name
```

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
as-path-name	Enter the name of an AS-PATH.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp filter-list hello` command shown in the Example below.

Field	Description
Path source codes	Lists the path sources shown to the right of the last AS number in the Path column: • i = internal route entry • a = aggregate route entry • c = external confederation route entry • n = network route entry • r = redistributed route entry
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
FTOS#show ip bgp filter-list hello
BGP table version is 80227, local router ID is 120.1.1.1
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n -
network
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network    Next Hop                Metric LocPrf Weight
Path
* I 6.1.5.0/24 192.100.11.2             20000   9999    0 ?
* I            192.100.8.2              20000   9999    0 ?
* I            192.100.9.2              20000   9999    0 ?
* I            192.100.10.2             20000   9999    0 ?
*>I            6.1.5.1                  20000   9999    0 ?
* I            6.1.6.1                  20000   9999    0 ?
* I            6.1.20.1                 20000   9999    0 ?
* I            6.1.6.0/24 192.100.11.2  20000   9999    0 ?
* I            192.100.8.2              20000   9999    0 ?
* I            192.100.9.2              20000   9999    0 ?
* I            192.100.10.2             20000   9999    0 ?
*>I            6.1.5.1                  20000   9999    0 ?
* I            6.1.6.1                  20000   9999    0 ?
* I            6.1.20.1                 20000   9999    0 ?
* I            6.1.20.0/24 192.100.11.2 20000   9999    0 ?
* I            192.100.8.2              20000   9999    0 ?
* I            192.100.9.2              20000   9999    0 ?
* I            192.100.10.2             20000   9999    0 ?
FTOS#
```

show ip bgp flap-statistics

View flap statistics on BGP routes.

S5000

Syntax

```
show ip bgp [ipv4 unicast] flap-statistics [ip-address [mask]]
[filter-list as-path-name] [regexp regular-expression]
```

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
ip-address	(OPTIONAL) Enter the IP address (in dotted decimal format) of the BGP network to view information only on that network.
mask	(OPTIONAL) Enter the network mask (in slash prefix (/x) format) of the BGP network address.
filter-list *as-path-name*	(OPTIONAL) Enter the keyword `filter-list` followed by the name of a configured AS-PATH ACL.
regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match:

- `.` = (period) any single character (including a white space).
- `*` = (asterisk) the sequences in a pattern (0 or more sequences).
- `+` = (plus) the sequences in a pattern (1 or more sequences).
- `?` = (question mark) sequences in a pattern (either 0 or 1 sequences).

  NOTE: You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression.
- `[ ]` = (brackets) a range of single-character patterns.
- `( )` = (parenthesis) groups a series of pattern elements to a single element.
- `{ }` = (braces) minimum and the maximum match count.
- `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp flap` command shown in the Example below.

Field	Description
Network	Displays the network ID to which the route is flapping.
From	Displays the IP address of the neighbor advertising the flapping route.
Flaps	Displays the number of times the route flapped.
Duration	Displays the hours:minutes:seconds since the route first flapped.
Reuse	Displays the hours:minutes:seconds until the flapped route is available.
Path	Lists all the ASs the flapping route passed through to reach the destination network.

Example

```
FTOS>show ip bgp flap
BGP table version is 210851, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
  r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

 Network      From      Flaps      Duration      Reuse
Path
FTOS>
```

show ip bgp inconsistent-as

View routes with inconsistent originating autonomous system (AS) numbers; that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

S5000

Syntax `show ip bgp [ipv4 unicast] inconsistent-as`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp inconsistent-as` command shown in the Example below.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.

Metric	Displays the BGP route’s metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route’s weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
FTOS>show ip bgp inconsistent-as
BGP table version is 280852, local router ID is 10.1.2.100
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, c - confed-external, r -
redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network Next  Hop         Metric LocPrf Weight Path
*  3.0.0.0/8     63.114.8.33                Ø 18508 209 7018
80 i
*                63.114.8.34                0 18508 209 7018
80 i
*                63.114.8.60                0 18508 209 7018
80 i
*>               63.114.8.33                0 18508 701 80 i
*> 3.18.135.0/24 63.114.8.60                0 18508 209 7018 ?
*                63.114.8.34                0 18508 209 7018 ?
*                63.114.8.33                0 18508 701 7018 ?
*                63.114.8.33                0 18508 209 7018 ?
*> 4.0.0.0/8     63.114.8.60                0 18508 209 1 i
*                63.114.8.34                0 18508 209 1 i
*                63.114.8.33                0 18508 701 1 i
*                63.114.8.33                0 18508 209 1 i
*  6.0.0.0/20    63.114.8.60                0 18508 209 3549 i
*                63.114.8.34                0 18508 209 3549 i
*>               63.114.8.33      0         0 18508 ?
*                63.114.8.33                0 18508 209 3549 i
*  9.2.0.0/16    63.114.8.60                0 18508 209 701 i
*                63.114.8.34                0 18508 209 701 i
--More--
```

show ip bgp neighbors

Allows you to view the information exchanged by BGP neighbors.

S5000

Syntax

`show ip bgp [`*`ipv4 unicast`*`] neighbors [`*`ip-address`*` [advertised-routes | dampened-routes | detail | flap-statistics | routes | {received-routes [`*`network`*` [`*`network-mask`*`]]} | {denied-routes [`*`network`*` [`*`network-mask`*`]]}]`

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.

ip-address	(OPTIONAL) Enter the IP address of the neighbor to view only BGP information exchanged with that neighbor.
advertised-routes	(OPTIONAL) Enter the keywords `advertised-routes` to view only the routes the neighbor sent.
dampened-routes	(OPTIONAL) Enter the keywords `dampened-routes` to view information on dampened routes from the BGP neighbor.
detail	(OPTIONAL) Enter the keyword `detail` to view neighbor-specific internal information for the IPv4 Unicast address family.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to view flap statistics on the neighbor's routes.
routes	(OPTIONAL) Enter the keyword `routes` to view only the neighbor's feasible routes.
received-routes [*network* [*network-mask*]	(OPTIONAL) Enter the keywords `received-routes` followed by either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information received from neighbors. **NOTE:** You must configure the `neighbor soft-reconfiguration inbound` command prior to viewing all the information received from the neighbors.
denied-routes [*network* [*network-mask*]	(OPTIONAL) Enter the keywords `denied-routes` followed by either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information on routes denied via neighbor inbound filters.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp neighbors` command shown in the Examples below.

Field	Description
BGP neighbor	Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, the link is internal; otherwise the link is external.
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information:

- last read is the time (hours:minutes:seconds) the router read a message from its neighbor
- hold time is the number of seconds configured between messages from its neighbor
- keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive.

Received messages	This line displays the number of BGP messages received, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Sent messages	The line displays the number of BGP messages sent, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Received updates	This line displays the number of BGP updates received and sent.
Soft reconfiguration	This line indicates that soft reconfiguration inbound is configured.
Minimum time	Displays the minimum time, in seconds, between advertisements.
(list of inbound and outbound policies)	Displays the policy commands configured and the names of the Route map, AS-PATH ACL, or Prefix list configured for the policy.
For address family:	Displays the IPv4 Unicast as the address family.
BGP table version	Displays which version of the primary BGP routing table the router and the neighbor are using.
accepted prefixes	Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.
Prefix advertised	Displays the number of network prefixes advertised, the number rejected, and the number withdrawn from the BGP routing table.
Connections established	Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.
Last reset	Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word never is displayed.
Local host:	Displays the peering address of the local router and the TCP port number.
Foreign host:	Displays the peering address of the neighbor and the TCP port number.

Example

```
FTOS#show ip bgp neighbors
BGP neighbor is 10.10.10.1, remote AS 23456, external link
  BGP version 4, remote router ID 10.10.10.1
  BGP state ESTABLISHED, in this state for 00:00:35
. . .
  Capabilities received from neighbor for IPv4 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    4_OCTECT_AS(65)
    ADD_PATH (69)
    CISCO_ROUTE_REFRESH(128)
```

Example

```
FTOS#show ip bgp neighbors

BGP neighbor is 100.10.10.2, remote AS 200, external link
  BGP version 4, remote router ID 192.168.2.101
  BGP state ESTABLISHED, in this state for 00:16:12
  Last read 00:00:12, last write 00:00:03
  Hold time is 180, keepalive interval is 60 seconds
Received 1404 messages, 0 in queue
  3 opens, 1 notifications, 1394 updates
  6 keepalives, 0 route refresh requests
 Sent 48 messages, 0 in queue
  3 opens, 2 notifications, 0 updates
  43 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds

  Capabilities received from neighbor for IPv4 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  Capabilities advertised to neighbor for IPv4 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    ROUTE_REFRESH(2)
    GRACEFUL_RESTART(64)
    CISCO_ROUTE_REFRESH(128)

  Route map for incoming advertisements is test
  Maximum prefix set to 4 with threshold 75

  For address family: IPv4 Unicast
  BGP table version 34, neighbor version 34
  5 accepted prefixes consume 20 bytes
  Prefix advertised 0, denied 4, withdrawn 0

Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
  Prefixes advertised 0, rejected 0, withdrawn 0 from peer

  Connections established 2; dropped 1
  Last reset 00:18:21, due to Maximum prefix limit reached
```

Example (Advertised-Routes)

```
FTOS>show ip bgp neighbors 192.14.1.5 advertised-routes

BGP table version is 74103, local router ID is 33.33.33.33
Status codes: s suppressed, S stale, d damped, h history, *
valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed,
n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network Next     Hop           Metric LocPrf  Weight Path
*>r 1.10.1.0/24     0.0.0.0        5000             32768 ?
*>r 1.11.0.0/16     0.0.0.0        5000             32768 ?
.....
...
```

```
*>I 223.94.249.0/24 223.100.4.249   0        100         0 ?
*>I 223.94.250.0/24 223.100.4.250   0        100         0 ?
*>I 223.100.0.0/16  223.100.255.254 0        100         0 ?
Total number of prefixes: 74102
```

Example (Received-Routes)

```
BGP table version is 13, local router ID is 120.10.10.1
Status codes: s suppressed, S stale, d damped, h history, *
valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed
n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network       Next Hop     Metric LocPrf   Weight Path
D   70.70.21.0/24 100.10.10.2             0   0 100 200 ?
D   70.70.22.0/24 100.10.10.2             0   0 100 200 ?
D   70.70.23.0/24 100.10.10.2             0   0 100 200 ?
D   70.70.24.0/24 100.10.10.2             0   0 100 200 ?
*>  70.70.25.0/24 100.10.10.2             0   0 100 200 ?
*>  70.70.26.0/24 100.10.10.2      0      0   0 100 200 ?
*>  70.70.27.0/24 100.10.10.2      0      0   0 100 200 ?
*>  70.70.28.0/24 100.10.10.2      0      0   0 100 200 ?
*>  70.70.29.0/24 100.10.10.2      0      0   0 100 200 ?
FTOS#
```

Example (denied-routes)

```
FTOS#show ip bgp neighbors 100.10.10.2 denied-routes
4 denied paths using 205 bytes of memory
BGP table version is 34, local router ID is 100.10.10.2
Status codes: s suppressed, S stale, d damped, h history, *
valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed
n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop     Metric LocPrf Weight Path
D  70.70.21.0/24  100.10.10.2             0    0 100 200 ?
D  70.70.22.0/24  100.10.10.2             0    0 100 200 ?
D  70.70.23.0/24  100.10.10.2             0    0 100 200 ?
D  70.70.24.0/24  100.10.10.2             0    0 100 200 ?
FTOS#
```

Related Commands

show ip bgp – views the current BGP routing table.

show ip bgp next-hop

View all next hops (using learned routes only) with current reachability and flap status. This command only displays one path, even if the next hop is reachable by multiple paths.

S5000

Syntax

```
show ip bgp next-hop
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp next-hop` command shown in the Example below.

Field	**Description**
Next-hop	Displays the next-hop IP address.
Via	Displays the IP address and interface used to reach the next hop.
RefCount	Displays the number of BGP routes using this next hop.
Cost	Displays the cost associated with using this next hop.
Flaps	Displays the number of times the next hop has flapped.
Time Elapsed	Displays the time elapsed since the next hop was learned. If the route is down, this field displays time elapsed since the route went down.

Example

```
FTOS>show ip bgp next-hop
  Next-hop    Via                  RefCount Cost Flaps Time
Elapsed
  63.114.8.33 63.114.8.33, Te 12/22   240984   0     0 00:18:25
  63.114.8.34 63.114.8.34, Te 12/22   135152   0     0 00:18:13
  63.114.8.35 63.114.8.35, Te 12/22        1   0     0 00:18:07
  63.114.8.60 63.114.8.60, Te 12/22   135155   0     0 00:18:11
FTOS>
```

show ip bgp paths

View all the BGP path attributes in the BGP database.

S5000

Syntax

`show ip bgp paths [regexp *regular-expression*]`

Parameters

regexp *regular-expression*

Enter a regular expression then use one or a combination of the following characters to match:

- `.` = (period) any single character (including a white space).
- `*` = (asterisk) the sequences in a pattern (0 or more sequences).
- `+` = (plus) the sequences in a pattern (1 or more sequences).
- `?` = (question mark) sequences in a pattern (either 0 or 1 sequences).

NOTE: You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression.

- `[ ]` = (brackets) a range of single-character patterns.
- `( )` = (parenthesis) groups a series of pattern elements to a single element.
- `{ }` = (braces) minimum and the maximum match count.
- `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp path` command shown in the Example below.

Field	Description
Total	Displays the total number of BGP path attributes.
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using this path attribute.
Metric	Displays the MED attribute for this path attribute.
Path	Displays the AS path for the route, with the origin code for the route listed last. Numbers listed between braces {} are AS_SET information.

Example

```
FTOS#show ip bgp path
Total 16 Paths
Address      Hash Refcount   Metric Path
0x1efe7e5c   15       10000          32 ?
0x1efe7e1c   71       10000          23 ?
0x1efe7ddc   127      10000          22 ?
0x1efe7d9c   183      10000          43 ?
0x1efe7d5c   239      10000          42 ?
0x1efe7c9c   283          6          {102 103} ?
0x1efe7b1c   287        336 20000    ?
0x1efe7d1c   295      10000          13 ?
0x1efe7c5c   339          6          {92 93} ?
0x1efe7cdc   351      10000          12 ?
0x1efe7c1c   395          6          {82 83} ?
0x1efe7bdc   451          6          {72 73} ?
0x1efe7b5c   491         78       0  ?
0x1efe7adc   883          2     120  i
0x1efe7e9c   983      10000          33 ?
0x1efe7b9c   1003         6       0  i
FTOS#
```

show ip bgp paths as-path

View all unique AS-PATHs in the BGP database.

S5000

Syntax `show ip bgp paths as-path`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp paths as-path` command shown in the Example below.

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these AS-Paths.
AS-Path	Displays the AS paths for this route, with the origin code for the route listed last. Numbers listed between braces {} are AS_SET information.

Example

```
FTOS#show ip bgp paths as-path
Total 13 AS-Paths
Address      Hash Refcount AS-Path
0x1ea3c1ec   251         1   42
0x1ea3c25c   251         1   22
0x1ea3c1b4   507         1   13
0x1ea3c304   507         1   33
0x1ea3c10c   763         1   {92 93}
0x1ea3c144   763         1   {102 103}
0x1ea3c17c   763         1   12
0x1ea3c2cc   763         1   32
0x1ea3c09c   764         1   {72 73}
0x1ea3c0d4   764         1   {82 83}
0x1ea3c224   1019        1   43
0x1ea3c294   1019        1   23
0x1ea3c02c   1021        4
FTOS#
```

show ip bgp paths community

View all unique COMMUNITY numbers in the BGP database.

S5000

Syntax `show ip bgp paths community`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp paths community` command shown in the Example below.

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these communities.
Community	Displays the community attributes in this BGP path.

Example

```
E1200-BGP>show ip bgp paths community
Total 293 Communities
Address      Hash   Refcount Community
0x1ec88a5c      3          4 209:209 209:6059 209:31272
3908:900 19092:300
0x1e0f10ec     15          4 209:209 209:3039 209:31272
3908:900 19092:300
0x1c902234     37          2 209:209 209:7193 209:21362
3908:900 19092:300
0x1f588cd4     41         24 209:209 209:6253 209:21362
3908:900 19092:300
0x1e805884     46          2 209:209 209:21226 286:777
286:3033 1899:3033
64675:21092
0x1e433f4c     46          8 209:209 209:5097 209:21362
3908:900 19092:300
0x1f173294     48         16 209:209 209:21226 286:40 286:777
286:3040 5606:40
12955:5606
0x1c9f8e24     50          6 209:209 209:4069 209:21362
3908:900 19092:300
0x1c9f88e4     53          4 209:209 209:3193 209:21362
3908:900 19092:300
0x1f58a944     57          6 209:209 209:2073 209:21362
3908:900 19092:300
0x1ce6be44     80          2 209:209 209:999 209:40832
0x1c6e2374     80          2 209:777 209:41528
0x1f58ad6c     82         46 209:209 209:41528
0x1c6e2064     83          2 209:777 209:40832
0x1f588ecc     85        570 209:209 209:40832
0x1f57cc0c     98          2 209:209 209:21226 286:3031
13646:1044 13646:1124
```

```
13646:1154 13646:1164 13646:1184 13646:1194 13646:1204
13646:1214 13646:1224
13646:1234 13646:1244 13646:1254 13646:1264 13646:3000
0x1d65b2ac     117         6 209:209 209:999 209:31272
0x1f5854ac     119        18 209:209 209:21226 286:108 286:111
286:777 286:3033
517:5104
```

show ip bgp peer-group

Allows you to view information on the BGP peers in a peer group.

S5000

Syntax

`show ip bgp [ipv4 unicast] peer-group [peer-group-name [detail | summary]]`

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
peer-group-name	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
detail	(OPTIONAL) Enter the keyword `detail` to view detailed status information of the peers in that peer group.
summary	(OPTIONAL) Enter the keyword `summary` to view status information of the peers in that peer group. The output is the same as that found in the `show ip bgp summary` command.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp peer-group` command shown in the Example below.

Lines beginning with	**Description**
Peer-group	Displays the peer group’s name.
Administratively shut	Displays the peer group’s status if the peer group is not enabled. If you enable the peer group, this line is not displayed.
BGP version	Displays the BGP version supported.
Minimum time	Displays the time interval between BGP advertisements.

For address family	Displays IPv4 Unicast as the address family.
BGP neighbor	Displays the name of the BGP neighbor.
Number of peers	Displays the number of peers currently configured for this peer group.
Peer-group members:	Lists the IP addresses of the peers in the peer group. If the address is outbound optimized, an * is displayed next to the IP address.

Example

```
FTOS#show ip bgp peer-group

Peer-group pg1
  BGP version 4
  Minimum time between advertisement runs is 30 seconds

  For address family: IPv4 Unicast
  BGP neighbor is pg1
Number of peers in this group 4
  Update packing has 4_OCTECT_AS support enabled
  Add-path support enabled
  Peer-group members (* - outbound optimized):
     1.1.1.5
     1.1.1.6
     10.10.10.2*
     20.20.20.100
```

Example

```
FTOS#show ip bgp peer-group

Peer-group RT-PEERS
Description: ***peering-with-RT***
BGP version 4
Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
BGP neighbor is RT-PEERS
Number of peers in this group 20
Peer-group members (* - outbound optimized):
  12.1.1.2*
  12.1.1.3*
  12.1.1.4*
  12.1.1.5*
  12.1.1.6*
  12.2.1.2*
  12.2.1.3*
  12.2.1.4*
  12.2.1.5*
  12.2.1.6*
  12.3.1.2*
  12.3.1.3*
  12.3.1.4*
  12.3.1.5*
  12.3.1.6*
  12.4.1.2*
  12.4.1.3*
  12.4.1.4*
  12.4.1.5*
  12.4.1.6*
```

Related Commands

neighbor peer-group (assigning peers) – assigns a peer to a peer-group.

neighbor peer-group (creating group) – creates a peer group.

show ip bgp peer-group (multicast) – views information on the BGP peers in a peer group.

show ip bgp regexp

Display the subset of the BGP routing table matching the regular expressions specified.

S5000

Syntax

```
show ip bgp regexp regular-expression [character]
```

Parameters

regular-expression [*character*]	Enter a regular expression then use one or a combination of the following characters to match: • `.` = (period) any single character (including a white space). • `*` = (asterisk) the sequences in a pattern (0 or more sequences). • `+` = (plus) the sequences in a pattern (1 or more sequences). • `?` = (question mark) sequences in a pattern (either 0 or 1 sequences). **NOTE:** You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression. • `[ ]` = (brackets) a range of single-character patterns. • `( )` = (parenthesis) groups a series of pattern elements to a single element. • `{ }` = (braces) minimum and the maximum match count. • `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified. • `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp regexp` command shown in the Example below.

Field	**Description**
Network	Displays the destination network prefix of each BGP route.

Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then non-BGP routes exist in the router's routing table.
Metric	Displays the BGP router's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the AS paths the route passed through to reach the destination network.

Example

```
FTOS#show ip bgp regexp ^2914+
BGP table version is 3700481, local router ID is 63.114.8.35
Status codes: s suppressed, S stale, d damped, h history, *
valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network       Next Hop   Metric LocPrf Weight Path
*>I 3.0.0.0/8     1.1.1.2         0 100         0 2914 1239 80
i
*>I 4.0.0.0/8     1.1.1.2         0 100         0 2914 3356 i
*>I 4.17.225.0/24 1.1.1.2         0 100         0 2914 11853
11853 11853 11853 11853 6496
*>I 4.17.226.0/23 1.1.1.2         0 100         0 2914 11853
11853 11853 11853 11853 6496
*>I 4.17.251.0/24 1.1.1.2         0 100         0 2914 11853
11853 11853 11853 11853 6496
*>I 4.17.252.0/23 1.1.1.2         0 100         0 2914 11853
11853 11853 11853 11853 6496
*>I 4.19.2.0/23   1.1.1.2         0 100         0 2914 701
6167 6167 6167 i
*>I 4.19.16.0/23  1.1.1.2         0 100         0 2914 701
6167 6167 6167 i
*>I 4.21.80.0/22  1.1.1.2         0 100         0 2914 174
4200 16559 i
*>I 4.21.82.0/24  1.1.1.2         0 100         0 2914 174
4200 16559 i
*>I 4.21.252.0/23 1.1.1.2         0 100         0 2914 701
6389 8063 19198 i
*>I 4.23.180.0/24 1.1.1.2         0 100         0 2914 3561
6128 30576 i
*>I 4.36.200.0/21 1.1.1.2         0 100         0 2914 14742
11854 14135 i
*>I 4.67.64.0/22  1.1.1.2         0 100         0 2914 11608
19281 i
*>I 4.78.32.0/21  1.1.1.2         0 100         0 2914 3491
29748 i
*>I 6.1.0.0/16    1.1.1.2         0 100         0 2914 701 668
i
*>I 6.2.0.0/22    1.1.1.2         0 100         0 2914 701 668
i
*>I 6.3.0.0/18    1.1.1.2         0 100         0 2914 701 668
i
```

show ip bgp summary

Allows you to view the status of all BGP connections.

S5000

Syntax	`show ip bgp [ipv4 unicast] summary`
Command Modes	- EXEC - EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp summary` command shown in the Example below.

Field	Description
BGP router identifier	Displays the local router ID and the AS number.
BGP table version	Displays the BGP table version and the main routing table version.
network entries	Displays the number of network entries, route paths, and the amount of memory used to process those entries.
paths	Displays the number of paths and the amount of memory used.
denied paths	Displays the number of denied paths and the amount of memory used.
BGP path attribute entries	Displays the number of BGP path attributes and the amount of memory used to process them.
BGP AS-PATH entries	Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.
BGP community entries	Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The `show ip bgp community` command provides more details on the COMMUNITY attributes.
Dampening enabled	Displayed only when you enable dampening. Displays the number of paths designated as history, dampened, or penalized.
Neighbor	Displays the BGP neighbor address.
AS	Displays the AS number of the neighbor.
MsgRcvd	Displays the number of BGP messages that neighbor received.
MsgSent	Displays the number of BGP messages that neighbor sent.
TblVer	Displays the version of the BGP table that was sent to that neighbor.
InQ	Displays the number of messages from that neighbor waiting to be processed.

OutQ	Displays the number of messages waiting to be sent to that neighbor. If a number appears in parentheses, the number represents the number of messages waiting to be sent to the peer group.
Up/Down	Displays the amount of time that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word never is displayed. The output format is shown below as Time Established with a display example: < 1 day 00:12:23 (hours:minutes:seconds) < 1 week 1d21h (DaysHours) > 1 week 11w2d (WeeksDays)
State/Pfxrcd	If the neighbor is in Established stage, the number of network prefixes received. If a maximum limit was configured with the `neighbor maximum-prefix` command, (prfxd) appears in this column. If the neighbor is not in Established stage, the current stage is displayed (Idle, Connect, Active, OpenSent, OpenConfirm). When the peer is transitioning between states and clearing the routes received, the phrase (Purging) may appear in this column. If the neighbor is disabled, the phrase (Admin shut) appears in this column.

Example

```
FTOS#show ip bgp summary
BGP router identifier 120.10.10.1, local AS number 100
BGP table version is 34, main routing table version 34
9 network entrie(s) using 1372 bytes of memory
5 paths using 380 bytes of memory
4 denied paths using 164 bytes of memory
BGP-RIB over all using 385 bytes of memory
2 BGP path attribute entrie(s) using 168 bytes of memory
1 BGP AS-PATH entrie(s) using 39 bytes of memory
1 BGP community entrie(s) using 43 bytes of memory
2 neighbor(s) using 7232 bytes of memory

Neighbor   AS  MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/
Pfx
100.10.10.2 200     46     41     34   0    0 00:14:33    5
120.10.10.2 300     40     47     34   0    0 00:37:10    0
FTOS#
```

show running-config bgp

Use this feature to display the current BGP configuration.

S5000

Syntax	`show running-config bgp`
Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

timers bgp

Adjust the BGP Keep Alive and Hold Time timers.

S5000

Syntax

`timers bgp keepalive holdtime`

To return to the default, use the `no timers bgp` command.

Parameters

keepalive	Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. The range is 1 to 65535. The default is **60 seconds**.
holdtime	Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. The range is 3 to 65535. The default is **180 seconds**.

Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the internet and connecting multicast topologies between BGP and autonomous systems (ASs).

FTOS MBGP is implemented as per IETF RFC 1858. BGPv4 is supported on the S5000 switch.

address family ipv4 multicast (MBGP)

This command changes the context to subsequent address family identifier (SAFI).

S5000

Syntax

`address family ipv4 multicast`

To remove SAFI context, use the `no address family ipv4 multicast` command.

Parameters

ipv4	Enter the keyword `ipv4` to specify the address family as IPV4.
multicast	Enter the keyword `multicast` to specify multicast as SAFI.

Defaults IPv4 Unicast

Command Modes ROUTER BGP (conf-router_bgp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

After you execute this command, all subsequent commands apply to this address family. You can exit from this AFI/SAFI to the IPv4 Unicast (the default) family by entering `exit` and returning to the Router BGP context.

aggregate-address

Summarize a range of prefixes to minimize the number of entries in the routing table.

S5000

Syntax

`aggregate-address` *`ip-address mask`* `[advertise-map` *`map-name`*`] [as-set] [attribute-map` *`map-name`*`] [summary-only] [suppress-map` *`map-name`*`]`

Parameters

ip-address mask	Enter the IP address and mask of the route to be the aggregate address. Enter the IP address in dotted decimal format (A.B.C.D) and mask in /prefix format (/x).
advertise-map *map-name*	(OPTIONAL) Enter the keywords `advertise-map` followed by the name of a configured route map to set filters for advertising an aggregate route.
as-set	(OPTIONAL) Enter the keyword `as-set` to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.

attribute-map *map-name*	(OPTIONAL) Enter the keywords `attribute-map` followed by the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
summary-only	(OPTIONAL) Enter the keyword `summary-only` to advertise only the aggregate address. Specific routes are not advertised.
suppress-map *map-name*	(OPTIONAL) Enter the keywords `suppress-map` followed by the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

If routes within the aggregate are constantly changing, do not add the `as-set` parameter to the aggregate as the aggregate flaps to keep track of the changes in the AS_PATH.

In route maps used in the `suppress-map` parameter, routes meeting the `deny` clause are not suppress; in other words, they are allowed. The opposite is also true; routes meeting the `permit` clause are suppressed.

If the route is injected via the `network` command, that route still appears in the routing table if the `summary-only` parameter is configured in the `aggregate-address` command.

The `summary-only` parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the `neighbor distribute-list` command.

bgp dampening

Enable MBGP route dampening.

S5000

Syntax

```
bgp dampening [half-life time] [route-map map-name]
```

To disable route dampening, use the `no bgp dampening [half-life time] [route-map map-name]` command.

Parameters

half-life time	(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half after the half-life period expires. The range is 1 to 45. The default is **15 minutes**.

route-map ***map-name***	(OPTIONAL) Enter the keyword `route-map` followed by the name of a configured route map. Only `match` commands in the configured route map are supported.

Defaults Disabled.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ip bgp ipv4 multicast

Reset MBGP sessions.

S5000

Syntax

```
clear ip bgp ipv4 multicast * ip-address [dampening | flap-
statistics] peer-group]
```

Parameters

*****	Enter an asterisk (*) to reset all BGP sessions.
ip-address	Enter an IP address in dotted decimal format to clear the prefixes from that neighbor.
dampening	(OPTIONAL) Enter the keyword `dampening` to clear route flap dampening information.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to reset the flap statistics on all prefixes from that neighbor.
peer-group	(OPTIONAL) Enter the keywords `peer-group` to clear all members of a peer-group.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ip bgp dampening

Clear information on route dampening.

S5000

Syntax

```
clear ip bgp dampening ipv4 multicast network network-mask
```

Parameters

dampening	Enter the keyword `dampening` to clear route flap dampening information.
network	(OPTIONAL) Enter the network address in dotted decimal format (A.B.C.D).
network-mask	(OPTIONAL) Enter the network mask in slash prefix format (/x).

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ip bgp flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

S5000

Syntax

```
clear ip bgp ipv4 multicast flap-statistics network | filter-list list |regexp regexp
```

Parameters

Network	(OPTIONAL) Enter the network address to clear flap statistics in dotted decimal format (A.B.C.D).
filter-list *as-path-name*	(OPTIONAL) Enter the keyword `filter-list` followed by the name of a configured AS-PATH list (maximum 16 characters).
regexp *regular-expression*	(OPTIONAL) Enter the keyword `regexp` followed by regular expressions. Use one or a combination of the following:

- `.` = (period) any single character (including a white space).
- `*` = (asterisk) the sequences in a pattern (0 or more sequences).
- `+` = (plus) the sequences in a pattern (1 or more sequences).
- `?` = (question mark) sequences in a pattern (either 0 or 1 sequences).

  NOTE: You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression.
- `[ ]` = (brackets) a range of single-character patterns.

- `( )` = (parenthesis) groups a series of pattern elements to a single element.
- `{ }` = (braces) minimum and the maximum match count.
- `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$` = (dollar sign) the end of the output string.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug ip bgp dampening

View information on routes being dampened.

S5000

Syntax

```
debug ip bgp ipv4 multicast dampening
```

To disable debugging, use the `no debug ip bgp ipv4 multicast dampening` command.

Parameters

dampening	Enter the keyword `dampening` to clear route flap dampening information.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ip bgp peer-group

Reset a peer-group’s BGP sessions.

S5000

Syntax

```
clear ip bgp peer-group peer-group-name
```

Parameters

peer-group-name	Enter the peer group name to reset the BGP sessions within that peer group.

Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

debug ip bgp updates

View information about BGP updates.

S5000

Syntax `debug ip bgp updates [in | out]`

To disable debugging, use the `no debug ip bgp updates [in | out]` command.

Parameters

updates	Enter the keyword `updates` to view BGP update information.
in	(OPTIONAL) Enter the keyword `in` to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view only BGP updates sent to neighbors.

Defaults	Disabled.
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

distance bgp

Configure three administrative distances for routes.

S5000

Syntax `distance bgp` *`external-distance internal-distance local-distance`*

To return to default values, use the `no distance bgp` command.

Parameters

external-distance	Enter a number to assign to routes learned from a neighbor external to the AS. The range is 1 to 255. The default is **20**.
internal-distance	Enter a number to assign to routes learned from a router within the AS. The range is 1 to 255. The default is **200**.
local-distance	Enter a number to assign to routes learned from networks listed in the network command. The range is 1 to 255. The default is **200**.

Defaults

- external-distance = **20**
- internal-distance = **200**
- local-distance = **200**

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

CAUTION: Dell Networking recommends not changing the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as internal BGP routes.

Related Commands

router bgp – enters ROUTER mode on the switch.

neighbor activate

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI.

S5000

Syntax

`neighbor [ip-address | peer-group-name] activate`

To disable, use the `no neighbor [ip-address | peer-group-name] activate` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group.
activate	Enter the keyword `activate` to enable the neighbor/peer group in the new AFI/SAFI.

Defaults Disabled

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

By default, when you create a neighbor/peer group configuration in the Router BGP context, this enables IPv4/Unicast AFI/SAFI. By using `activate` in the new context, the neighbor/peer group enables for AFI/SAFI.

Related Commands	address family ipv4 multicast (MBGP) – changes the context to SAFI.

neighbor advertisement-interval

Set the advertisement interval between BGP neighbors or within a BGP peer group.

S5000

Syntax

`neighbor {ip-address | peer-group-name} advertisement-interval seconds`

To return to the default value, use the `no neighbor {ip-address | peer-group-name} advertisement-interval` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
seconds	Enter a number as the time interval, in seconds, between BGP advertisements. The range is 0 to 600 seconds. The default is **5 seconds** for internal BGP peers and **30 seconds** for external BGP peers.

Defaults

- seconds = **5 seconds** (internal peers)
- seconds = **30 seconds** (external peers)

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Command History

Version 9.0(1.3)	Introduced on the S5000.

neighbor default-originate

Inject the default route to a BGP peer or neighbor.

S5000

Syntax

`neighbor {ip-address | peer-group-name} default-originate [route-map map-name]`

To remove a default route, use the `no neighbor {ip-address | peer-group-name} default-originate` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the default route of all routers in that peer group.
route-map *map-name*	(OPTIONAL) Enter the keyword `route-map` followed by the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Command History

Version 9.0(1.3)	Introduced on the S5000.

neighbor distribute-list

Distribute BGP information using an established prefix list.

S5000

Syntax

```
neighbor [ip-address | peer-group-name] distribute-list prefix-list-name [in | out]
```

To delete a neighbor distribution list, use the `no neighbor [ip-address | peer-group-name] distribute-list prefix-list-name [in | out]` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to apply the distribute list filter to all routers in the peer group.
prefix-list-name	Enter the name of an established prefix list. If the prefix list is not configured, the default is **permit** (to allow all routes).
in	Enter the keyword `in` to distribute only inbound traffic.
out	Enter the keyword `out` to distribute only outbound traffic.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Other BGP filtering commands include: `neighbor filter-list`, `ip as-path access-list`, and `neighbor route-map`.

Related Commands	ip as-path access-list – configures the IP AS-Path ACL. neighbor filter-list – assigns a AS-PATH list to a neighbor or peer group. neighbor route-map – assigns a route map to a neighbor or peer group.

neighbor filter-list

Configure a BGP filter based on the AS-PATH attribute.

S5000

Syntax

```
neighbor [ip-address | peer-group-name] filter-list aspath
access-list-name [in | out]
```

To delete a BGP filter, use the `no neighbor [ip-address | peer-group-name] filter-list aspath access-list-name [in | out]` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to apply the filter to all routers in the peer group.
as-path-name	Enter the name of an established AS-PATH access list (up to 140 characters). If the AS-PATH access list is not configured, the default is **permit** (allow routes).
in	Enter the keyword `in` to filter inbound BGP routes.
out	Enter the keyword `out` to filter outbound BGP routes.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Use the `ip as-path access-list` command in CONFIGURATION mode to enter AS-PATH ACL mode and configure the AS-PATH filters to deny or permit BGP routes based on information in their AS-PATH attribute.

Related Commands ip as-path access-list – enter AS-PATH ACL mode and configure the AS-PATH filters.

neighbor maximum-prefix

Control the number of network prefixes received.

S5000

Syntax

`neighbor {ip-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]`

To return to the default values, use the `no neighbor {ip-address | peer-group-name} maximum-prefix maximum` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
maximum	Enter a number as the maximum number of prefixes allowed for this BGP router. The range is 1 to 4294967295.
threshold	(OPTIONAL) Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches this percentage of the maximum value, the S5000 software sends a message. The range is 1 to 100 percent. The default is **75**.
warning-only	(OPTIONAL) Enter the keyword `warning-only` to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

Defaults

threshold = **75**

Command Modes

ROUTER BGP Address Family (conf-router_bgp_af)

Command History

Version 9.0(1.3)	Introduced on the S5000.

neighbor next-hop-self

Allows you to configure the router as the next hop for a BGP neighbor.

S5000

Syntax

`neighbor {ip-address | peer-group-name} next-hop-self`

To return to the default setting, use the `no neighbor {ip-address | peer-group-name} next-hop-self` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.

Defaults Disabled.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Command History

Version 9.0(1.3)	Introduced on the S5000.

neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

S5000

Syntax `neighbor {ip-address | peer-group-name} remove-private-as`

To return to the default, use the `no neighbor {ip-address | peer-group-name} remove-private-as` command.

Parameters

ip-address	Enter the IP address of the neighbor to remove the private AS numbers.
peer-group-name	Enter the name of the peer group to remove the private AS numbers.

Defaults Disabled (that is, private AS numbers are not removed).

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Command History

Version 9.0(1.3)	Introduced on the S5000.

neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

S5000

Syntax `neighbor {ip-address | peer-group-name} route-map map-name {in | out}`

To remove the route map, use the `no neighbor {ip-address | peer-group-name} route-map map-name {in | out}` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
map-name	Enter the name of an established route map.

	If the Route map is not configured, the default is **deny** (to drop all routes).
in	Enter the keyword `in` to filter inbound routes.
out	Enter the keyword `out` to filter outbound routes.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

Configure a neighbor as a member of a route reflector cluster.

S5000

Syntax `neighbor {`*`ip-address`*` | `*`peer-group-name`*`} route-reflector-client`

To indicate that the neighbor is not a route reflector client or to delete a route reflector configuration, use the `no neighbor `*`ip-address`*` | `*`peer-group-name`*` route-reflector-client` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The first time you enter this command, it configures the neighbor as a route reflector and members of the route-reflector cluster. If you configure a route reflector, internal BGP (IBGP) speakers do not need to be fully meshed.

When you disable all clients of a route reflector, the neighbor is no longer a route reflector.

network

Specify the networks for the BGP process and enter them in the BGP routing table.

S5000

Syntax

`network ip-address mask [route-map map-name]`

To remove a network, use the `no network ip-address mask [route-map map-name]` command.

Parameters

ip-address	Enter an IP address in dotted decimal format of the network.
mask	Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).
route-map *map-name*	(OPTIONAL) Enter the keyword `route-map` followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ip address • set community • set local-preference • set metric • set next-hop • set origin • set weight If the route map is not configured, the default is **deny** (to drop all routes).

Defaults

Not configured.

Command Modes

ROUTER BGP Address Family (conf-router_bgp_af)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

FTOS software resolves the network address configured by the `network` command with the routes in the main routing table to ensure that the networks are reachable using non-BGP routes and non-default routes.

Related Commands

redistribute – redistributes routes into the BGP.

redistribute

Redistribute routes into BGP.

S5000

Syntax	`redistribute [connected | static] [route-map map-name]` To disable redistribution, use the `no redistribution [connected | static] [route-map map-name]` command.
Parameters	

connected	Enter the keyword `connected` to redistribute routes from physically connected interfaces.
static	Enter the keyword `static` to redistribute manually configured routes. These routes are treated as incomplete routes.
route-map *map-name*	(OPTIONAL) Enter the keyword `route-map` followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ip address • set community • set local-preference • set metric • set next-hop • set origin • set weight If the route map is not configured, the default is **deny** (to drop all routes).

Defaults	Not configured.
Command Modes	ROUTER BGP Address Family (conf-router_bgp_af)
Command History	

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	If you do not configure the `default-metric` command, in addition to the `redistribute` command, or there is no route map to set the metric, the metric for redistributed static and connected is “0”. To redistribute the default route (0.0.0.0/0), configure the `neighbor default-originate` command.
Related Commands	neighbor default-originate – injects the default route.

redistribute ospf

Redistribute OSPF routes into BGP.

S5000

Syntax	`redistribute ospf` *`process-id`* `[[match external {1	2}] [match internal]] [route-map` *`map-name`*`]` To stop redistribution of OSPF routes, use the `no redistribute ospf` *`process-id`* command.
Parameters	

process-id	Enter the number of the OSPF process. The range is 1 to 65535.
match external {1 | 2}	(OPTIONAL) Enter the keywords `match external` to redistribute OSPF external routes. You can specify `1` or `2` to redistribute those routes only.
match internal	(OPTIONAL) Enter the keywords `match internal` to redistribute OSPF internal routes only.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of a configured route map.

Defaults	Not configured.
Command Modes	ROUTER BGP Address Family (conf-router_bgp_af)
Command History	

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	When you enter the `redistribute isis` *`process-id`* command without any other parameters, FTOS redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes. This feature is not supported by an RFC. This feature is not supported by an RFC.

show ip bgp ipv4 multicast

View the current MBGP routing table for the system.

S5000

Syntax	`show ip bgp ipv4 multicast [detail |` *`network`* `[`*`network-mask`*`] [length]]`
Parameters	

detail	(OPTIONAL) Enter the keyword `detail` to display BGP internal information for the IPv4 Multicast address family.
network	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.

network-mask	(OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.
longer-prefixes	(OPTIONAL) Enter the keywords `longer-prefixes` to view all routes with a common prefix.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you enable the `bgp non-deterministic-med` command, the `show ip bgp` command output for a BGP route does not list the INACTIVE reason.

The following describes the `show ip bgp ipv4 multicast` command shown the Example below.

Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route’s metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route’s weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
FTOS#show ip bgp ipv4 multicast
BGP table version is 14, local router ID is 100.10.10.1
Status codes: s suppressed, S stale, d damped, h history, *
valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network        Next Hop       Metric  LocPrf Weight Path
*>I 25.1.0.0/16    25.25.25.25        0     100      0 i
*>I 25.2.0.0/16    25.25.25.26        0     100      0 ?
*>I 25.3.0.0/16    211.1.1.165        0     100      0 ?
*>r 144.1.0.0/16   0.0.0.0 0                      32768 ?
*>r 144.2.0.0/16   100.10.10.10       0           32768 ?
*>r 144.3.0.0/16   211.1.1.135        0           32768 ?
*>n 145.1.0.0/16   0.0.0.0 0                      32768 i
FTOS#
```

Related Commands

show ip bgp community – views the BGP communities.

show ip bgp cluster-list

View BGP neighbors in a specific cluster.

S5000

Syntax

```
show ip bgp ipv4 multicast cluster-list [cluster-id]
```

Parameters

cluster-id	(OPTIONAL) Enter the cluster id in dotted decimal format.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp community

View information on all routes with Community attributes or view specific BGP community groups.

S5000

Syntax

```
show ip bgp ipv4 multicast community [community-number] [local-
as] [no-export] [no-advertise]
```

Parameters

community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.
local-AS	Enter the keywords `local-AS` to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords `no-advertise` to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords `no-export` to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp` command output.

show ip bgp community-list

View routes that are affected by a specific community list.

S5000

Syntax

```
show ip bgp ipv4 multicast community-list community-list-name
```

Parameters

community-list-name	Enter the name of a configured IP community list (max 16 characters).

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp dampened-paths

View BGP routes that are dampened (non-active).

S5000

Syntax

```
show ip bgp [ipv4 unicast] dampened-paths
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp damp` command shown in the Example below.

Field	**Description**
Network	Displays the network ID to which the route is dampened.
From	Displays the IP address of the neighbor advertising the dampened route.
Reuse	Displays the hour:minutes:seconds until the dampened route is available.
Path	Lists all the ASs the dampened route passed through to reach the destination network.

Example

```
FTOS>show ip bgp damp
BGP table version is 210708, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network      From       Reuse       Path
FTOS>
```

show ip bgp filter-list

View the routes that match the filter lists.

S5000

Syntax

```
show ip bgp ipv4 multicast filter-list as-path-name
```

Parameters

as-path-name	Enter the name of an AS-PATH.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp flap-statistics

View flap statistics on BGP routes.

S5000

Syntax

```
show ip bgp ipv4 multicast flap-statistics [ip-address [mask]]
[filter-list as-path-name] [regexp regular-expression]
```

Parameters

ip-address	(OPTIONAL) Enter the IP address (in dotted decimal format) of the BGP network to view information only on that network.
mask	(OPTIONAL) Enter the network mask (in slash prefix (/x) format) of the BGP network address.
filter-list *as-path-name*	(OPTIONAL) Enter the keyword `filter-list` followed by the name of a configured AS-PATH ACL.
regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match: • `.` = (period) any single character (including a white space). • `*` = (asterisk) the sequences in a pattern (0 or more sequences). • `+` = (plus) the sequences in a pattern (1 or more sequences). • `?` = (question mark) sequences in a pattern (either 0 or 1 sequences). **NOTE:** You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression. • `[ ]` = (brackets) a range of single-character patterns. • `( )` = (parenthesis) groups a series of pattern elements to a single element. • `{ }` = (braces) minimum and the maximum match count. • `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified. • `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp inconsistent-as

View routes with inconsistent originating AS numbers; that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

S5000

Syntax

```
show ip bgp ipv4 multicast inconsistent-as
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp ipv4 multicast neighbors

Allows you to view the information exchanged by BGP neighbors.

S5000

Syntax

```
show ip bgp ipv4 multicast neighbors [ip-address [advertised-
routes | dampened-routes | detail | flap-statistics | routes]]
```

Parameters

ip-address	(OPTIONAL) Enter the IP address, in either IPv4 or IPv6 format, of the neighbor to view only BGP information exchanged with that neighbor.
advertised-routes	(OPTIONAL) Enter the keywords `advertised-routes` to view only the routes the neighbor sent.
dampened-routes	(OPTIONAL) Enter the keywords `dampened-routes` to view information on dampened routes from the BGP neighbor.
detail	(OPTIONAL) Display detailed neighbor information.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to view flap statistics on the neighbor's routes.
routes	(OPTIONAL) Enter the keyword `routes` to view only the neighbor's feasible routes.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp ipv4 multicast neighbors` command shown in the Example below.

BGP neighbor	Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, then the link is internal; otherwise the link is external.
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information: • last read is the time (hours:minutes:seconds) the router read a message from its neighbor • hold time is the number of seconds configured between messages from its neighbor • keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive.
Received messages	This line displays the number of BGP messages received, the number of notifications (error messages) and the number of messages waiting in a queue for processing.
Sent messages	The line displays the number of BGP messages sent, the number of notifications (error messages) and the number of messages waiting in a queue for processing.
Received updates	This line displays the number of BGP updates received and sent.
Minimum time	Displays the minimum time, in seconds, between advertisements.
(list of inbound and outbound policies)	Displays the policy commands configured and the names of the Route map, AS-PATH ACL or Prefix list configured for the policy.
For address family:	Displays IPv4 Unicast as the address family.
BGP table version	Displays the which version of the primary BGP routing table the router and the neighbor are using.
accepted prefixes	Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.
Prefix advertised	Displays the number of network prefixes advertised, the number rejected and the number withdrawn from the BGP routing table.
Connections established	Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.
Last reset	Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word never is displayed.

Local host:	Displays the peering address of the local router and the TCP port number.
Foreign host:	Displays the peering address of the neighbor and the TCP port number.

Example

```
FTOS#show ip bgp ipv4 multicast neighbors
BGP neighbor is 25.25.25.25, remote AS 6400, internal link
  BGP version 4, remote router ID 25.25.25.25
  BGP state ESTABLISHED, in this state for 00:02:18
  Last read 00:00:16, hold time is 180, keepalive interval is
60 seconds
Received 1404 messages, 0 in queue
    3 opens, 1 notifications, 1394 updates
    6 keepalives, 0 route refresh requests
  Sent 48 messages, 0 in queue
    3 opens, 2 notifications, 0 updates
    43 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 5 seconds
Minimum time before advertisements start is 0 seconds
  Capabilities received from neighbor for IPv4 unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)
  Capabilities advertised to neighbor for IPv4 Multicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)
  Update source set to Loopback 0
  For address family: IPv4 Multicast
  BGP table version 14, neighbor version 14
  3 accepted prefixes consume 12 bytes
Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
  Prefixes advertised 0, rejected 0, withdrawn 0 from peer
Connections established 2; dropped 1
  Last reset 00:03:17, due to user reset

  Notification History
    'Connection Reset' Sent : 1 Recv: 0

Local host: 100.10.10.1, Local port: 179
Foreign host: 25.25.25.25, Foreign port: 2290

BGP neighbor is 211.1.1.129, remote AS 640, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state ACTIVE, in this state for 00:00:36
  Last read 00:00:41, hold time is 180, keepalive interval is
60 seconds
  Received 28 messages, 0 notifications, 0 in queue
  Sent 6 messages, 3 notifications, 0 in queue
  Received 18 updates, Sent 6 updates
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

  For address family: IPv4 Multicast
  BGP table version 14, neighbor version 0
  0 accepted prefixes consume 0 bytes
  Prefix advertised 0, rejected 0, withdrawn 0

  Connections established 3; dropped 3
  Last reset 00:00:37, due to user reset
```

```
Notification History
  'Connection Reset' Sent : 3 Recv: 0
```

Related Commands

show ip bgp – views the current BGP routing table.

show ip bgp peer-group

Allows you to view information on the BGP peers in a peer group.

S5000

Syntax

`show ip bgp ipv4 multicast peer-group [peer-group-name [detail | summary]]`

Parameters

peer-group-name	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
detail	(OPTIONAL) Enter the keyword `detail` to view detailed status information of the peers in that peer group.
summary	(OPTIONAL) Enter the keyword `summary` to view status information of the peers in that peer group. The output is the same as that found in the `show ip bgp summary` command.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

neighbor peer-group (assigning peers) – assigns a peer to a peer-group.

neighbor peer-group (creating group) – creates a peer group.

show ip bgp peer-group (multicast) – views information on the BGP peers in a peer group.

show ip bgp summary

Allows you to view the status of all BGP connections.

S5000

Syntax

`show ip bgp ipv4 multicast summary`

Command Modes	- EXEC - EXEC Privilege

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Usage Information

The following describes the `sho ip bgp ipv4 multicast summary` command shown in the Example below.

BGP router identifier	Displays the local router ID and the AS number.
BGP table version	Displays the BGP table version and the main routing table version.
network entries	Displays the number of network entries, route paths, and the amount of memory used to process those entries.
BGP path attribute entries	Displays the number of BGP path attributes and the amount of memory used to process them.
BGP AS-PATH entries	Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.
BGP community entries	Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The `show ip bgp community` command provides more details on the COMMUNITY attributes.
Dampening enabled	Displayed only when you enable dampening. Displays the number of paths designated as history, dampened, or penalized.
Neighbor	Displays the BGP neighbor address.
AS	Displays the AS number of the neighbor.
MsgRcvd	Displays the number of BGP messages that neighbor received.
MsgSent	Displays the number of BGP messages that neighbor sent.
TblVer	Displays the version of the BGP table that was sent to that neighbor.
InQ	Displays the number of messages from that neighbor waiting to be processed.
OutQ	Displays the number of messages waiting to be sent to that neighbor. If a number appears in parentheses, the number represents the number of messages waiting to be sent to the peer group.
Up/Down	Displays the amount of time (in hours:minutes:seconds) that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word never is displayed.
State/Pfxrcd	If the neighbor is in Established stage, the number of network prefixes received. If a maximum limit was configured with the `neighbor maximum-prefix` command, (prfxd) appears in this column. If the neighbor is not in Established stage, the current stage is displayed (Idle, Connect, Active, OpenSent, OpenConfirm). When the

peer is transitioning between states and clearing the routes received, the phrase (Purging) may appear in this column.

If the neighbor is disabled, the phrase (Admin shut) appears in this column.

Example

```
FTOS#sho ip bgp ipv4 multicast summary
BGP router identifier 100.10.10.1, local AS number 6400
BGP table version is 14, main routing table version 14
7 network entrie(s) and 7 paths using 972 bytes of memory
2 BGP path attribute entrie(s) using 112 bytes of memory
1 BGP AS-PATH entrie(s) using 35 bytes of memory

Neighbor      AS   MsgRcvd MsgSent TblVer InQ OutQ Up/Down
State/Pfx
25.25.25.25   6400      21       9     14   0    0
00:02:04        3
211.1.1.129   640       28       6      0   0    0 00:00:21
Active
FTOS#
```

BGP Extended Communities (RFC 4360)

BGP Extended Communities, as defined in RFC 4360, is an optional transitive BGP attribute.

BGP Extended Communities provides two major advantages over Standard Communities:

- The range is extended from 4-octet (AA:NN) to 8-octet (Type:Value) to provide enough number communities.
- Communities are structured using a new “Type” field (1 or 2-octets), allowing you to provide granular control/filter routing information based on the type of extended communities.

deny

Use this feature to reject (deny) from the two types of extended communities, route origin (rt) or site-of-origin (soo).

S5000

Syntax

`deny {rt | soo} {as4 ASN4:NN | ASN:NNNN | IPADDR:NN}`

To remove (delete) the rule, use the `no deny {rt | soo} {as4 ASN4:NN | ASN:NNNN | IPADDR:NN}` command.

Parameters

rt	Enter the keyword `rt` to designate a Route Origin community.
soo	Enter the keyword `soo` to designate a Site-of-Origin community (also known as Route Origin).
as4 ***ASN4:NN***	Enter the keyword `as4` followed by the 4-octet AS specific extended community number in the format ASN4:NN (4-byte AS number:2-byte community value).

ASN:NNNN	Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).
IPADDR:NN	Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value).

Defaults Not configured.

Command Modes CONFIGURATION (conf-ext-community-list)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

permit – configures to add (permit) rules.

show ip extcommunity-list – displays the extended community list.

deny regex

This features allows you to specify an extended communities to reject (deny) using a regular expressions (regex).

S5000

Syntax `deny regex {regex}`

To remove, use the `no deny regex {regex}` command.

Parameters

regex	Enter a regular expression.

Defaults Not configured.

Command Modes CONFIGURATION (conf-ext-community-list)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Duplicate commands are silently accepted.

Example

```
FTOS(conf-ext-community-list)#deny regexp 123
FTOS(conf-ext-community-list)#
```

Related Commands

permit regex – permits a community using a regular expression.

description

Use this feature to designate a meaningful description to the extended community.

S5000

Syntax

`description {line}`

To remove the description, use the `no description {line}` command.

Parameters

line	Enter a description (maximum 80 characters).

Defaults Not configured.

Command Modes CONFIGURATION (conf-ext-community-list)

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip extcommunity-list

Use this feature to enter the Extended Community-list mode.

S5000

Syntax

`ip extcommunity-list word`

To exit from this mode, use the `exit` command.

Parameters

word	Enter a community list name (maximum 16 characters).

Defaults none

Command Modes CONFIGURATION (conf-ext-community-list)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This mode changes the prompt.

Example

```
FTOS(conf)#ip extcommunity-list test
FTOS(conf-ext-community-list)#
```

match extcommunity

Use this feature to match an extended community in the Route Map mode.

S5000

Syntax `match extcommunity {`*`extended community list name`*`}`

To change the match, use the `no match extcommunity {`*`extended community list name`*`}` command.

Parameters

extended community list name	Enter the name of the extended community list.

Defaults none

Command Modes ROUTE MAP (config-route-map)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Like standard communities, you can use extended communities in the route-map to match the attribute.

Example

```
FTOS(config-route-map)#match extcommunity Freedombird
FTOS(config-route-map)#
```

permit

Use this feature to add rules (permit) from the two types of extended communities, Route Origin (rt) or Site-of-Origin (soo).

S5000

Syntax `permit {rt | soo} {as4 `*`ASN4:NN`*` | `*`ASN:NNNN`*` | `*`IPADDR:NN`*`}`

To change the rules, use the `no permit {rt | soo} {as4 `*`ASN4:NN`*` | `*`ASN:NNNN`*` | `*`IPADDR:NN`*`}` command.

Parameters

rt	Enter the keyword `rt` to designate a Route Origin community.
soo	Enter the keyword `soo` to designate a Site-of-Origin community (also known as Route Origin).
as4 ***ASN4:NN***	Enter the keyword `as4` followed by the 4-octet AS specific extended community number in the format ASN4:NN (4-byte AS number:2-byte community value).
ASN:NNNN	Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).

IPADDR:NN	Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value).

Defaults Not configured.

Command Modes CONFIGURATION (conf-ext-community-list)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

deny – configures to delete (deny) rules.

show ip bgp extcommunity-list – displays the extended community list.

permit regex

This features allows you specify an extended communities to forward (permit) using a regular expressions (regex).

S5000

Syntax `permit regex {`*`regex`*`}`

To remove, use the `no permit regex {`*`regex`*`}` command.

Parameters

regex	Enter a regular expression.

Defaults Not configured.

Command Modes CONFIGURATION (conf-ext-community-list)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Duplicate commands are silently accepted.

Example

```
FTOS(conf-ext-community-list)#permit regexp 123
FTOS(conf-ext-community-list)#
```

Related Commands deny regex – denies a community using a regular expression.

set extcommunity rt

Use this feature to set Route Origin community attributes in Route Map.

S5000

Syntax

```
set extcommunity rt {as4 ASN4:NN [non-trans] | ASN:NNNN [non-trans] | IPADDR:NN [non-trans]} [additive]
```

To delete the Route Origin community, use the `no set extcommunity` command.

Parameters

as4 *ASN4:NN*	Enter the keyword `as4` followed by the 4-octet AS specific extended community number in the format ASN4:NN (4-byte AS number:2-byte community value).
ASN:NNNN	Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).
IPADDR:NN	Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value).
additive	(OPTIONAL) Enter the keyword `additive` to add to the existing extended community.
non-trans	(OPTIONAL) Enter the keywords `non-trans` to indicate a non-transitive BGP extended community.

Defaults

none

Command Modes

ROUTE MAP (config-route-map)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If the set community `rt` and `soo` are in the same route-map entry, the behavior defines as:

- If the `rt` option comes before `soo`, with or without the `additive` option, `soo` overrides the communities set by `rt`.
- If the `rt` option comes after `soo`, without the `additive` option, `rt` overrides the communities set by `soo`.
- If the `rt` with the `additive` option comes after `soo`, `rt` adds the communities set by `soo`.

Related Commands

set extcommunity soo – sets the extended community site-of-origin in the route-map.

set extcommunity soo

Use this feature to set extended community site-of-origin in Route Map.

S5000

Syntax

`set extcommunity soo {as4 ASN4:NN | ASN:NNNN | IPADDR:NN [non-trans]}`

To delete the site-of-origin community, use the `no set extcommunity` command.

Parameters

as4 ***ASN4:NN***	Enter the keyword `as4` followed by the 4-octet AS specific extended community number in the format ASN4:NN (4-byte AS number:2-byte community value).
ASN:NNNN	Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).
IPADDR:NN	Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value).
non-trans	(OPTIONAL) Enter the keywords `non-trans` to indicate a non-transitive BGP extended community.

Defaults

none

Command Modes

ROUTE MAP (config-route-map)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If the set community `rt` and `soo` are in the same route-map entry, the behavior defines as:

- If the `rt` option comes before `soo`, with or without the `additive` option, `soo` overrides the communities set by `rt`.
- If the `rt` option comes after `soo`, without the `additive` option, `rt` overrides the communities set by `soo`.
- If the `rt` with the `additive` option comes after `soo`, `rt` adds the communities set by `soo`.

Related Commands

set extcommunity rt – sets the extended community route origins using the route-map.

show ip bgp ipv4 extcommunity-list

Use this feature to display the IPv4 routes matching the extended community list name.

S5000

Syntax

```
show ip bgp [ipv4 [multicast | unicast] | ipv6 unicast]
extcommunity-list name
```

Parameters

multicast	Enter the keyword `multicast` to display the multicast route information.
unicast	Enter the keyword `unicast` to display the unicast route information.
ipv6 unicast	Enter the keywords `ipv6 unicast` to display the IPv6 unicast route information.
name	(OPTIONAL) Enter the name of the extcommunity-list.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If there is a type or sub-type that is not well-known, it is displayed as:`TTSS:XX:YYYY`.

Where TT is type, SS is sub-type displayed in hexadecimal format, XX:YYYY is the value divided into 2-byte and 4-byte values in decimal format. This format is consistent with other vendors.

For example, if the extended community has type 0x04, sub-type 0x05, value 0x20 00 00 00 10 00, it displays as:`0x0405:8192:4096`.

Non-transitive extended communities are marked with an asterisk.

Example

```
FTOS#show ip bgp ipv4 multicast extcommunity-list
BGP routing table entry for 192.168.1.0/24, version 2

Paths: (1 available, table Default-IP-Routing-Table.)
Not advertised to any peer
Received from :
  100.100.1.2 (2.4.0.1) Best
    AS_PATH : 200
    Next-Hop : 100.100.1.2, Cost : 0
    Origin IGP, Metric 4294967295 (Default), LocalPref 100,
Weight 0,
external
    Communities :
    300:400 500:600

    Extended Communities :
    RT:1111:4278080 SoO:35:4 SoO:36:50529043 SoO:37:50529044
    SoO:38:50529045 SoO:0.0.0.2:33 SoO:506.62106:34
0x0303:254:11223*
```

```
FTOS#
```

show ip bgp paths extcommunity

Use this feature to display all BGP paths having extended community attributes.

S5000

Syntax `show ip bgp paths extcommunity`

Parameters

The following describes the `show ip bgp paths extcommunity` command shown in the Example below.

Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these extended communities.
Community	Displays the extended community attributes in this BGP path.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip bgp paths extcommunity
Total 1 Extended Communities

Address      Hash  Refcount Extended Community
0x41d57024   12272 1        RT:7:200 SoO:5:300 SoO:0.0.0.3:1285

FTOS#
```

show ip extcommunity-list

Display the IP extended community list.

S5000

Syntax `show ip extcommunity-list [`*`word`*`]`

Parameters		
	word	Enter the name of the extended community list you want to view.

Command Modes

- EXEC
- EXEC Privilege

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip extcommunity-list test
ip extcommunity-list test
  deny RT:1234:12
  permit regexp 123
  deny regexp 234
  deny regexp 123
FTOS#
```

show running-config extcommunity-list

Use this feature to display the current configuration of the extended community lists.

S5000

Syntax `show running-config extcommunity-list [word]`

Parameters		
	word	Enter the name of the extended community list you want to view.

Defaults none

Command Modes EXEC Privilege

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show running-config extcommunity-list test

ip extcommunity-list test
  permit rt 65033:200
  deny soo 101.11.11.2:23
  permit rt as4 110212:340
  deny regex ^(65001_)$

FTOS#
```

11

Bare Metal Provisioning (BMP)

Bare metal provisioning (BMP) version 2.0 is supported on the S5000 switch.

In a data center network, BMP automates the configuration and updating of switches, ensuring standard configurations across the installed devices.

You can configure auto-configuration on a single switch or on multiple switches. BMP allows you to set up a stack with a minimum of effort, but is also useful for quick configuration of a single switch.

For additional information about BMP in Auto-Configuration mode, refer to the *Open Automation Guide*.

BMP 2.0 eases configuration by providing the following key features:

- Boot images and running configurations are specified in a DHCP server.
- Files are automatically downloaded from a file server and applied by the switch
- Switch access is allowed through all ports (management and user ports) with or without DHCP-based dynamic IP address configuration of a switch.
- Booting up in Layer 3 mode with interfaces already in No Shutdown mode and only enabling some basic protocols to protect the system and the network

reload type

BMP 2.0 AutoCconfiguration mode: Configure a switch to reload in Normal mode or as a DHCP client with all ports configured for Layer 3 traffic.

S5000

Syntax

```
reload-type {normal-reload | jump-start [config-download
{enable | disable}] [dhcp-timeout minutes]}
```

Parameters

normal-reload	The switch reloads in Normal mode using the FTOS image and startup configuration file stored in the local flash
jump-start	The switch reloads in Jumpstart mode as a DHCP client.
config-download {enable | disable}	(Optional) Configure whether the switch boots up using the configuration file downloaded from the DHCP/file servers (enable) OR if the downloaded file will be discarded and the startup configuration file stored in the local flash will be used (disable).
dhcp-timeout *minutes*	(Optional) Configure the DHCP timeout (in minutes) after which the Jumpstart reload stops. The range is 1 to 50. The default is **Infinite number of retries**.

Defaults A switch running BMP 2.0 reloads in Jumpstart mode as a DHCP client with all ports configured for Layer 3 traffic.

Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced for the S5000.
Usage Information	For an initial setup, the `config-download` parameter of the `reload-type` command is enabled. After the configuration file is successfully downloaded, the `config-download` parameter is automatically disabled. You can enable it again using the `reload-type` command. After you set Auto-Configuration mode (Jumpstart or Normal reload) using the `reload-type` command, you must enter the reload command to reload the switch in the Configured mode. When a switch reloads in Jumpstart mode, all ports, including the management port, are automatically configured as Layer 3 physical ports. The switch acts as a DHCP client on the ports for a user-configured time (the `dhcp-timeout` option). You can reconfigure the default startup configuration and DHCP timeout values. If a switch enters a loop while reloading in Jumpstart mode because the switch continuously tries to contact a DHCP server and a DHCP server is not found, enter the `stop jump-start` command to interrupt the reload and boot up in Normal mode. The startup configuration is then loaded from the local flash on the switch. Use the `reload-type` command in BMP 2.0 to toggle between Normal and Jumpstart Auto-Configuration modes. The reload settings for Auto-Configuration mode that you configure are stored in memory and retained for future reboots and BMP software upgrades. You can enter the `reload` command at any time to reload the switch in the last configured mode: Normal reload or Jumpstart mode.
Related Commands	• show reload-type – displays the current reload mode (Normal or jump-start mode). • stop jump-start – stops the Jumpstart process to prevent a loop if the DHCP server is not found.

show reload-type

Display the reload type currently configured on the system.

S5000

Syntax	`show reload-type`
Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced for the S5000.
Usage Information	Use the `show reload-type` command to check the currently configured Auto-Configuration mode (Jumpstart or Normal reload) on a switch running BMP 2.0.

You can also use the `show bootvar` command to display the current Reload mode for BMP 2.0 with the path of the FTOS image file retrieved from a DHCP server.

Example

```
FTOS#show reload-type

Reload-Type : normal-reload [Next boot : normal-reload]
```

Related Commands

reload type – configures Reload mode as normal or Jumpstart.

stop jump-start

Stop the switch from reloading in Jumpstart mode to prevent an infinite loop.

S5000

Syntax

```
stop jump-start
```

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced for the S5000.

Usage Information

Use the `stop jump-start` command on a switch running BMP 2.0 if the switch enters a loop while reloading in Jumpstart mode; loop occurs when the switch is continuously trying to contact a DHCP server and a DHCP server is not found. The `stop jump-start` command stops the switch from connecting to the DHCP server. After you use the `stop jump-start` command, the next default reload type is a normal reload. This is indicated in the `show reload-type` command.

Related Commands

reload type – configures Rload mode as normal or Jumpstart.

12

Content Addressable Memory (CAM)

Content addressable memory (CAM) commands are supported on the S5000 switch.

CAM Profile Commands

The CAM profiling feature allows you to partition the CAM to best suit your application. For example:

- Configure more Layer 2 ACL entries when the system is deployed as a switch.
- Configure more Layer 3 ACL entries when the system is deployed as a router.
- Configure more FCoE or iSCSI ACLs to handle an increase in storage traffic.

Important Points to Remember

- The CAM configuration is applied to the entire system when you use the CONFIGURATION mode commands. You must save the running-configuration to affect the change.
- When budgeting your CAM allocations for ACLs and quality of service (QoS) configurations, remember that ACL and QoS rules might consume more than one CAM entry depending on complexity. For example, transmission control protocol (TCP) and user datagram protocol (UDP) rules with `port range` options might require more than one CAM entry.
- You MUST save your changes and reboot the system for CAM profiling or allocations to take effect.

cam-acl (Configuration)

Reset CAM allocation to default settings or reconfigure CAM allocation for Layer 2, IPv4, and IPv6 ACLs, Layer 2 and Layer 3 (IPv4) QoS, Layer 2 Protocol Tunneling (L2PT), IP and MAC source address validation for DHCP, Ethernet Connectivity Fault Management (CFM) ACLs, and (optionally) FCoE and iSCSI ACLs.

S5000

Syntax

```
cam-acl {default | l2acl number ipv4acl number ipv6acl number
ipv4qos number l2qos number l2pt number ipmacacl number ecfmacl
number {vman-qos number | vman-dual-qos number} [fcoeacl
number] [iscsioptacl number]}
```

Parameters

default Use the default CAM profile settings and set the CAM as follows:

- L2 ACL(l2acl): 5
- L3 ACL (ipv4acl): 4
- IPv6 L3 ACL (ipv6acl): 0

- L3 QoS (ipv4qos): 1
- L2 QoS (l2qos): 1
- L2PT (l2pt): 0
- MAC ACLs (ipmacacl): 0
- ECFMACL (ecfmacl): 0
- VMAN QoS (vman-qos): 0
- VMAN Dual QoS (vman-dual-qos): 0
- FCoE ACL (fcoeacl): 2
- iSCSI Opt ACL (iscsioptacl): 0

l2acl *number* ipv4acl *number* ipv6acl *number*ipv4qos *number* l2qos *number*l2pt *number* ipmacacl *number* ecfmacl *number* {vman-qos *number* | vman-dual-qos *number*} [fcoeacl *number*][iscsiacl *number*]

Enter the number fo FP blocks to be allocated to each CAM region. Separate each keyword and number with a blank space. the total allocated CAM space must equal 13.

The ipv6acl and vman–dual–qos allocations must be entered as a factor of 2 (2, 4, 6, 8, or 10). All other CAM regions can use either even or odd numbered numbers.

The range of memory blocks that you can allocate to each CAM region is 0 to 10.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Clarified block information for the S5000.

Usage Information

You must save the new CAM settings to the startup-config (`write-mem` or `copy run start`) then reload the system for the new settings to take effect.

The total amount of CAM space allowed is 16 FP Blocks. System flow requires three blocks; these blocks cannot be reallocated. Therefore, the total number of allocated blocks for all CAM regions must be 13.

cam-acl-egress (Configuration)

Select the FP groups for CAM access control lists for Layer 2, IPv4, and IPv6 ACLs.

S5000

Syntax

```
cam-acl-egress {default | l2acl number ipv4acl number ipv6acl
number}
```

Parameters

default	Reset the egress CAM ACL entries to the default settings.
l2acl *number* **ipv4acl** *number* **ipv6acl** *number*	Allocate space to each CAM region. Enter the CAM profile name followed by the amount of CAM space to be allotted. The total space allocated must equal 13. The l2acl range is 1 to 4. The ipv4acl range is 1 to 4. The ipv6acl range is 0 to 4.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must save the new CAM settings to the startup-config (`write-mem` or `copy run start`) then reload the system for the new settings to take effect.

There are four groups total. You must allocate at least one group for L2ACL and IPv4 ACL.

The range for the CAM profiles are 1 to 4 for l2acl. The range for the `ipv6acl` profile is 0 to 10. The `ipv6acl` allocation must be a factor of 2 (2, 4, 6, 8, 10).

cam-optimization

Optimize CAM utilization for QoS Entries by minimizing require policy-map CAM space.

S5000

Syntax `cam-optimization [qos]`

Parameters

qos	Optimize CAM usage for QoS.

Defaults Disabled.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you enable this command, if a Policy Map containing classification rules (ACL and/or dscp/ ip-precedence rules) is applied to more than one physical interface on the same port pipe, only a single copy of the policy is written (only one FP entry is used).

NOTE: An ACL itself may still require more that a single FP entry, regardless of the number of interfaces. For more information, refer to the “IP Access Control Lists”, “Prefix Lists”, and “Route-map” sections in the *FTOS Configuration Guide*.

test cam-usage

Verify that enough CAM space is available for the ingress IPv4 ACLs used in a QoS policy.

S5000

Syntax

```
test cam-usage service-policy input policy-map-name policy-map
name stack-unit [ unit-number | all ]}
```

Parameters

policy-map name	Enter the name of the policy-map to verify.
stack-unit *unit-number*	Enter the keyword `stack-unit` followed by a number. The range is 0 to 11.
stack-unit all	Enter the keyword `stack-unit` followed by a `all` to get information for all the stack-units.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command applies to the IPv4 CAM region and is best used to verify QoS optimization for IPv4 ACLs.

QoS Optimization for IPv4 ACLs does not impact the CAM usage for applying a policy on a single (or the first of several) interfaces. It is most useful when a policy is applied across multiple interfaces; it can reduce the impact to CAM usage across subsequent interfaces.

Usage Information

The following describes output for the `test cam-usage` command shown in the Example below.

Column Heading	Explanation
Stack-Unit	Lists specified stack unit(s) or all of them.
Portpipe	Lists the portpipe (port-set) or port pipes (port-sets) that are checked. Entering `all` shows the status for all stack-units and port-pipes in the chassis.
CAM Partition	Shows the CAM profile of the CAM.
Available CAM	Identifies the amount of CAM space remaining for that profile.
Estimated CAM per Port	Estimates the amount of CAM space the listed policy will require.
Status	Indicates whether or not the policy will be allowed in the CAM.

Example

```
FTOS#test cam-usage service-policy input TestIn stack-unit all

Stack-Unit|Portpipe|CAM Partition|AvailableCAM|EstimatedCAM
per Port|Status
--------------------------------------------------------------
         0|       0|      IPv4Flow|
102|                    0|Allowed
         0|       1|     IPv4Flow|
102|                    0|Allowed
FTOS#
!
FTOS#test cam-usage service-policy input TestIn stack-unit 0 port-set 0

Stack-Unit|Portpipe|CAM Partition|Available CAM|EstimatedCAM
per Port|Status
---------------------------------------------------------------
--
         0|       1|     IPv4Flow|
102|                    0|Allowed
FTOS#
```

13

Control Plane Policing (CoPP)

The CoPP commands are supported on the S5000 switch.

control-plane-cpuqos

Enter control-plane mode and configure the switch to manage control-plane traffic.

S5000

Syntax	`control-plane-cpuqos`
Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.

service-policy rate-limit-cpu-queues

Apply a policy map for the system to rate limit control traffic on a per-queue basis.

S5000

Syntax	`service-policy rate-limit-cpu-queues` *`policy-name`*
Parameters	***policy-name*** Enter the service-policy name, using a string up to 140 characters.
Defaults	Not configured.
Command Modes	CONTROL-PLANE-CPUQOS
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	You must create a policy-map by associating a queue number with the qos-policy. You must create QoS policies prior to enabling this command.

Related Commands	qos-policy-input – creates a QoS input policy map. class-map – creates a QoS class map. policy-map-input – creates an input policy map.

service-policy rate-limit-protocols

Apply a policy for the system to rate limit control protocols on a per-protocol basis.

S5000

Syntax

```
service-policy rate-limit-protocols policy-name
```

Parameters

policy-name	Enter the service-policy name, using a string up to 140 characters.

Defaults	Not configured.
Command Modes	CONTROL-PLANE-CPUQOS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command applies the service-policy based on the type of protocol defined in the ACL rules.

You must create ACL and QoS policies prior to enabling this command.

Related Commands	ip access-list extended – creates an extended IP ACL. ipv6 access-list – creates an IPv6 ACL. mac access-list extended – creates an extended MAC ACL. qos-policy-input – creates a QoS input policy map. class-map – creates a QoS class map. policy-map-input – creates an input policy map.

show cpu-queue rate cp

Display the rates for each queue.

S5000

Syntax

```
show cpu-queue rate cp
```

Defaults	Not configured.
Command Modes	EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command applies the service-policy based on the type of protocol defined in the ACL rules.

You must create ACL and QoS policies prior to enabling this command.

Example

```
FTOS#show cpu-queue rate cp
Service-Queue Rate (PPS)
-------------- -----------
Q0                1300
Q1                300
Q2                300
Q3                300
Q4                2000
Q5                400
Q6                400
Q7                1100
FTOS#
```

show ip protocol-queue-mapping

Display the queue mapping for each configured protocol.

S5000

Syntax `show ip protocol-queue-mapping`

Defaults Not configured.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip protocol-queue-mapping
Protocol    Src-Port    Dst-Port   TcpFlag   Queue EgPort
Rate(kbps)
----     --------    --------   ------- ----- ------
-----------
TCP (BGP)     any/179      179/any       _      Q6     CP
100
UDP (DHCP)    67/68        68/67         _      Q6/Q5  CP     _
UDP (DHCP-R)  67           67            _      Q6     CP     _
TCP (FTP)     any          21            _      Q6     CP     _
ICMP          any          any           _      Q6     CP     _
IGMP          any          any           _      Q7     CP     _
TCP (MSDP)    any/639      639/any       _      Q6     CP     _
UDP (NTP)     any          123           _      Q6     CP     _
OSPF          any          any           _      Q7     CP     _
PIM           any          any           _      Q7     CP     _
UDP (RIP)     any          520           _      Q7     CP     _
TCP (SSH)     any          22            _      Q6     CP     _
TCP (TELNET)  any          23            _      Q6     CP     _
```

```
VRRP          any          any            _      Q7      CP      _
FTOS#
```

show ipv6 protocol-queue-mapping

Display the queue mapping for each configured IPv6 protocol.

S5000

Syntax `show ipv6 protocol-queue-mapping`

Defaults Not configured.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ipv6 protocol-queue-mapping
Protocol    Src-Port   Dst-Port  TcpFlag Queue EgPort
Rate(kbps)
--------    --------   --------  ------- ----- ------ --------
TCP (BGP)    any/179     179/any    _      Q6     CP     _
ICMP         any         any        _      Q6     CP     _
VRRP         any         any        _      Q7     CP     _

FTOS#
```

show mac protocol-queue-mapping

Display the queue mapping for the MAC protocols.

S5000

Syntax `show mac protocol-queue-mapping`

Defaults Not configured.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show mac protocol-queue-mapping
Protocol Destination Mac        EtherType Queue EgPort
Rate(kbps)
----------------------------------- ----- ------ -----------
ARP        any                     0x0806   Q5/Q6  CP       _
FRRP       01:01:e8:00:00:10/11    any      Q7     CP       _
LACP       01:80:c2:00:00:02       0x8809   Q7     CP       _
```

```
LLDP       any                     0x88cc   Q7      CP       _
GVRP       01:80:c2:00:00:21       any      Q7      CP       _
STP        01:80:c2:00:00:00       any      Q7      CP       _
ISIS       01:80:c2:00:00:14/15    any      Q7      CP       _
           09:00:2b:00:00:04/05    any      Q7      CP
FTOS#
```

14

Data Center Bridging (DCB)

Data center bridging (DCB) refers to a set of IEEE Ethernet enhancements that provide data centers with a single, robust, converged network to support multiple traffic types, including local area network (LAN), server, and storage traffic.

FTOS commands for data center bridging features include 802.1Qbb priority-based flow control (PFC), 802.1Qaz enhanced transmission selection (ETS), and the data center bridging exchange (DCBx) protocol.

This chapter includes the following sections:

- DCB Command
- PFC Commands
- ETS Commands
- DCBx Commands

DCB Command

The following DCB command is supported on the S5000 platform.

advertise dcbx-appln-tlv

On a DCBx port with a manual role, configure the application priority TLVs advertised on the interface to DCBx peers.

S5000

Syntax	`advertise dcbx-appln-tlv {fcoe | iscsi}` To remove the application priority TLVs, use the `no advertise dcbx-appln-tlv {fcoe | iscsi}` command.
Parameters	**{fcoe | iscsi}** Enter the application priority TLVs, where: • `fcoe`: enables the advertisement of FCoE in application priority TLVs. • `iscsi`: enables the advertisement of iSCSI in application priority TLVs.
Defaults	Application priority TLVS are enabled to advertise FCoE and iSCSI.
Command Modes	PROTOCOL LLDP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To disable TLV transmission, use the `no` form of the command; for example, `no advertise dcbx-appln-tlv iscsi`.

advertise dcbx-tlv

On a DCBx port with a manual role, configure the PFC and ETS TLVs advertised to DCBx peers.

S5000

Syntax

```
advertise dcbx-tlv {ets-conf | ets-reco | pfc} [ets-conf | ets-
reco | pfc] [ets-conf | ets-reco | pfc]
```

To remove the advertised ETS TLVs, use the `no advertise dcbx-tlv` command.

Parameters

{ets-conf | ets-reco | pfc}	Enter the PFC and ETS TLVs advertised, where: • `ets-conf`: enables the advertisement of ETS configuration TLVs. • `ets-reco`: enables the advertisement of ETS recommend TLVs. • `pfc`: enables the advertisement of PFC TLVs.

Defaults

All PFC and ETS TLVs are advertised.

Command Modes

PROTOCOL LLDP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can configure the transmission of more than one TLV type at a time; for example: `advertise dcbx-tlv ets-conf ets-reco`.

You can enable ETS recommend TLVs (`ets-reco`) only if you enable ETS configuration TLVs (`ets-conf`). To disable TLV transmission, use the `no` form of the command; for example, `no advertise dcbx-tlv pfc ets-reco`.

DCBx requires that you enable LLDP to advertise DCBx TLVs to peers.

Configure DCBx operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBx configuration on a port, use the `show interface dcbx detail` command.

clear ets counters

Clear all ETS TLV counters on an interface.

S5000

Syntax

```
clear ets counters interface-type slot/port
```

Parameters

interface-type slot/port	Enter one of the following interface types and slot/port information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear pfc counters

Clear the PFC TLV counters and PFC statistics on an interface or stack unit.

S5000

Syntax

```
clear pfc counters {[interface-type slot/port | stack-unit]
[unit-number | all ] [stack-ports all]}
```

Parameters

interface-type slot/port	Enter one of the following keywords and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
stack-unit ***unit-number***	Enter the keyword `stack-unit` followed by a number. The range is 0 to 11.

	stack-unit all stack-ports all	Enter the keyword `stack-unit` followed by `all stack-ports all` to clear the counters on all interfaces.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

dcb enable

Enable data center bridging.

S5000

Syntax `dcb enable`

To disable DCB, use the `no dcb-enable` command.

Defaults Enabled

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

By default, DCB is enabled and link-level flow control is disabled on all S5000 interfaces.

To disable DCB, enter the `no dcb enable` command.

Related Commands

dcb-map– creates a DCB map to configure PFC and ETS parameters and apply the PFC and ETS settings on Ethernet ports.

dcb-map

Create a DCB map to configure priority flow control (PFC) and enhanced transmission selection (ETS) on Ethernet ports that support converged Ethernet traffic. Apply the DCB map to an Ethernet interface.

S5000

Syntax `dcb-map` *`map-name`*

Parameters

map-name	Enter a DCB map name. The maximum number of alphanumeric characters is 32.

Defaults None. There are no pre-configured PFC and ETS settings on S5000 Ethernet interfaces.

Command Modes	CONFIGURATION INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Usage Information

A DCB map is a template used to configure DCB parameters and apply them on converged Ethernet interfaces. DCB parameters include priority-based flow control (PFC) and enhanced traffic selection (ETS).

To display the PFC and ETS settings in DCB maps, enter the `show qos dcb-map` command.

Use the `dcb-map` command to create a DCB map to specify PFC and ETS settings and apply it on Ethernet ports. After you apply a DCB map to an interface, the PFC and ETS settings in the map are applied when the Ethernet port is enabled. DCBx is enabled on Ethernet ports by default.

The `dcb-map` command is supported only on physical Ethernet interfaces.

To remove a DCB map from an interface, enter the `no dcb-map` *`map-name`* command in Interface configuration mode.

Related Commands

show qos dcb-map– displays the dcb-map profiles configured on the system.

dcb-map stack-unit all stack-ports all– applies a DCB map on all ports of a switch stack.

dcb-map stack-unit all stack-ports all

Apply the specified DCB map on all ports of the switch stack.

S5000

Syntax

`dcb-map stack-unit all stack-ports all` *`dcb-map-name`*

To remove the PFC and ETS settings in a DCB map from all stack units, use the `no dcb-map stack-unit all stack-ports all` command.

Parameters

dcb-map-name	Enter the name of the DCB map.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `dcb-map stack-unit all stack-ports all` command overwrites any previous DCB maps applied to stack ports.

Related Commands

dcb-map – creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports.

dcbx port-role

Configure the DCBx port role the interface uses to exchange DCB information.

S5000

Syntax

```
dcbx port-role {auto-downstream | auto-upstream | config-source
| manual}
```

To remove a DCBx port role, use the `no dcbx port-role {auto-downstream | auto-upstream | config-source | manual}` command.

Parameters

auto-downstream | auto-upstream | config-source | manual	Enter the DCBx port role, where: • `auto-upstream`: configures the port to receive a peer configuration. The configuration source is elected from auto-upstream ports. • `auto-downstream`: configures the port to accept the internally propagated DCB configuration from a configuration source. • `config-source`: configures the port to serve as the configuration source on the switch. • `manual`: configures the port to operate only on administer-configured DCB parameters. The port does not accept a DCB configuration received form a peer or a local configuration source.

Defaults Manual

Command Modes INTERFACE PROTOCOL LLDP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

DCBx requires that you enable LLDP to advertise DCBx TLVs to peers.

Configure DCBx operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBx configuration on a port, use the `show interface dcbx detail` command.

dcbx version

Configure the DCBx version used on the interface.

S5000

Syntax

```
dcbx version {auto | cee | cin | ieee-v2.5}
```

To remove the DCBx version, use the `dcbx version {auto | cee | cin | ieee-v2.5}` command.

Parameters

auto | cee | cin | ieee-v2.5	Enter the DCBx version type used on the interface, where: • `auto`: configures the port to operate using the DCBx version received from a peer. • `cee`: configures the port to use CEE (Intel 1.01). • `cin`: configures the port to use Cisco-Intel-Nuova (DCBx 1.0). • `ieee-v2.5`: configures the port to use IEEE 802.1az (Draft 2.5).

Defaults Auto

Command Modes INTERFACE PROTOCOL LLDP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

DCBx requires that you enable LLDP to advertise DCBx TLVs to peers.

Configure DCBx operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBx configuration on a port, use the `show interface dcbx detail` command.

debug dcbx

Enable DCBx debugging.

S5000

Syntax

```
debug dcbx {all | auto-detect-timer | config-exchng | fail |
mgmt | resource | sem | tlv}
```

To disable DCBx debugging, use the `no debug dcbx` command.

Parameters

{all | auto-detect-timer | config-exchng | fail | mgmt | resource | sem | tlv}	Enter the type of debugging, where: • `all`: enables all DCBx debugging operations. • `auto-detect-timer`: enables traces for DCBx auto-detect timers. • `config-exchng`: enables traces for DCBx configuration exchanges. • `fail`: enables traces for DCBx failures. • `mgmt`: enables traces for DCBx management frames. • `resource`: enables traces for DCBx system resource frames. • `sem`: enables traces for the DCBx state machine. • `tlv`: enables traces for DCBx TLVs.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

fcoe priority-bits

Configure the FCoE priority advertised for the FCoE protocol in application priority TLVs.

S5000

Syntax `fcoe priority-bits` *`priority-bitmap`*

To remove the configured FCoE priority, use the `no fcoe priority-bits` command.

Parameters

priority-bitmap	Enter the priority-bitmap range. The range is 1 to FF.

Defaults 0x8

Command Modes PROTOCOL LLDP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This command is available at the global level only.

iscsi priority-bits

Configure the iSCSI priority advertised for the iSCSI protocol in application priority TLVs.

S5000

Syntax `iscsi priority-bits` *`priority-bitmap`*

To remove the configured iSCSI priority, use the `no iscsi priority-bits` command.

Parameters

priority-bitmap	Enter the priority-bitmap range. The range is 1 to FF.

Defaults 0x10

Command Modes PROTOCOL LLDP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	This command is available at the global level only.

pfc mode on

Re-enable or disable PFC operation in a DCB map applied to an Ethernet port.

S5000

Syntax	`pfc mode on` To disable PFC configuration in a DCB map, use the `no pfc mode on` command.
Defaults	PFC mode is on.
Command Modes	DCB MAP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	By default, PFC is enabled on S5000 Ethernet ports and 802.1p priorities are included in DCBx negotiation with peer PFC devices Use the `no pfc mode on` command in a DCB map and apply the map to an interface to disable PFC before you configure lossless queues on a port on which PFC is not required. To configure lossless queues, use the `pfc no-drop queues` command To re-enable PFC operation on an interface, open the DCB map for editing (`dcb-map` command), enter the `pfc mode on` command, and re-apply the map on the interface. You cannot enable PFC and link-level flow control at the same time on an interface.
Related Commands	dcb-map – creates a DCB map to configure PFC and ETS parameters and apply the PFC and ETS settings on Ethernet ports.

pfc no-drop queues

Configure the port queues that still function as no-drop queues for lossless traffic.

S5000

Syntax	`pfc no-drop queues` *`queue-range`* To remove the no-drop port queues, use the `no pfc no-drop queues` command.
Parameters	***queue-range*** Enter the queue range. Separate the queue values with a comma; specify a priority range with a dash; for example, `pfc no-drop queues 1,3` or `pfc no-drop queues 2-3`. The range is 0 to 3.

Defaults

No lossless queues are configured.

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The configuration of no-drop queues provides flexibility for ports on which PFC is not needed but lossless traffic should egress from the interface.

The maximum number of lossless queues supported per port is two.

The default dot1p priority-queue mapping is:

dot1p Value in Incoming Frame	Egress Queue
0	0
1	0
2	0
3	1
4	2
5	3
6	3
7	3

pfc priority

Enable PFC on 802.1p priority traffic without using a DCB map.

S5000

Syntax

`pfc priority` *`priority-range`*

To delete the pfc priority configuration, use the `no pfc priority` command.

Parameters

priority-range	Enter the 802.1p values of the frames to be paused. Separate the priority values with a comma; specify a priority range with a dash; for example, pfc priority 3,5-7. The range is 0 to 7.

Defaults

none

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	Use the `pfc priority` command to configure PFC operation on an Ethernet interface for specified CoS traffic without using a DCB map in a network topology that uses the default ETS setting (assigns equal bandwidth to each 802.1p priority). The maximum number of lossless queues supported per port is two. If you reconfigure the lossless queues for no-drop priorities in a DCB map and reapply the map to the interface, traffic may be interrupted due to an interface flap (going down and coming up). The maximum number of lossless queues supported per port is two. A PFC peer must support the configured priority traffic (as detected by DCBx) to apply PFC.
Related Commands	dcb-map — creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports.

priority-group bandwidth pfc

Configure the ETS bandwidth allocation and PFC mode used to manage port traffic in an 802.1p priority group.

S5000

Syntax

```
priority-group group-num {bandwidth percentage| strict-
priority} pfc {on | off}
```

Parameters

priority-group *group-num*	Enter the keyword `priority-group` followed by the number of an 802.1p priority group. Use the `priority-pgid` command to create the priority groups in a DCB map.
bandwidth *percentage*	Enter the keyword `bandwidth` followed by a bandwidth percentage allocated to the priority group. The range of valid values is 1 to 100. The sum of all allocated bandwidth percentages in priority groups in a DCB map must be 100%.
strict-priority	Configure the priority-group traffic to be handled with strict priority scheduling. Strict-priority traffic is serviced first, before bandwidth allocated to other priority groups is made available.
pfc {on | off}	Configure whether priority-based flow control is enabled (on) or disabled (off) for port traffic in the priority group.

Defaults	None
Command Modes	DCB MAP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Use the `dcb-map` command to configure priority groups with PFC and/or ETS settings and apply them to Ethernet interfaces. Use the `priority-pgid` command to map 802.1p priorities to a priority group. You can assign each 802.1p priority to only one priority group. A priority group consists of 802.1p priority values that are grouped together for similar bandwidth allocation and scheduling, and that

share latency and loss requirements. All 802.1p priorities mapped to the same queue must be in the same priority group.

Repeat the `priority-group bandwidth pfc` command to configure PFC and ETS traffic handling for each priority group in a DCB map.

You can enable PFC on a maximum of two priority queues.

If you configure more than one priority group as strict priority, the higher numbered priority queue is given preference when scheduling data traffic.

If a priority group does not use its allocated bandwidth, the unused bandwidth is made available to other priority groups.

To remove a priority-group configuration in a DCB map, enter the `no priority-group bandwidth pfc` command.

By default, equal bandwidth is assigned to each dot1p priority in a priority group. Use the `bandwidth` parameter to configure the bandwidth percentage assigned to a priority group. The sum of the bandwidth allocated to all priority groups in a DCB map must be 100% of the bandwidth on the link. You must allocate at least 1% of the total port bandwidth to each priority group.

Related Commands

dcb-map – creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports.

priority-pgid – configures the 802.1p priority traffic in a priority group for a DCB map.

priority-pgid

Assign 802.1p priority traffic to a priority group in a DCB map.

S5000

Syntax

```
priority-pgid dot1p0_group-num dot1p1_group-num dot1p2_group-
num dot1p3_group-num dot1p4_group-num dot1p5_group-num
dot1p6_group-num dot1p7_group-num
```

Parameters

dot1p0_group-num	Enter the priority group number for each 802.1p class of traffic in a DCB map.
dot1p1_group-num	
dot1p2_group-num	
dot1p3_group-num	
dot1p4_group-num	
dot1p5_group-num	

	dot1p6_group-num *dot1p7_group-num*
Defaults	None
Command Modes	DCB MAP
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Usage Information

PFC and ETS settings are not pre-configured on Ethernet ports. You must use the `dcb-map` command to configure different groups of 802.1p priorities with PFC and ETS settings.

Using the `priority-pgid` command, you assign each 802.1p priority to one priority group. A priority group consists of 802.1p priority values that are grouped together for similar bandwidth allocation and scheduling, and that share latency and loss requirements. All 802.1p priorities mapped to the same queue must be in the same priority group. For example, the `priority-pgid 0 0 0 1 2 4 4 4` command creates the following groups of 802.1p priority traffic:

- Priority group 0 contains traffic with dot1p priorities 0, 1, and 2.
- Priority group 1 contains traffic with dot1p priority 3.
- Priority group 2 contains traffic with dot1p priority 4.
- Priority group 4 contains traffic with dot1p priority 5, 6, and 7.

To remove a priority-pgid configuration from a DCB map, enter the `no priority-pgid` command.

Related Commands

dcb-map — creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports.

priority-group bandwidth pfc— configures the ETS bandwidth allocation and the PFC setting used to manage the port traffic in an 802.1p priority group.

show dcb

Displays the data center bridging status.

S5000

Syntax	`show dcb`
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
FTOS# show dcb
      DCB Status : Enabled
FTOS#
```

show qos dcb-map

Display the DCB parameters configured in a specified DCB map.

S5000

Syntax

```
show qos dcb-map map-name
```

Parameters

map-name	Displays the PFC and ETS parameters configured in the specified map.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `show qos dcb-map` command to display the enhanced transmission selection (ETS) and priority-based flow control (PFC) parameters used to configure server-facing Ethernet ports. S5000 Ethernet ports are DCBx-enabled by default.

The following table describes the `show qos dcb-map` output shown in the example below.

Field	Description
State	Complete: All mandatory DCB parameters are correctly configured. In progress: The DCB map configuration is not complete. Some mandatory parameters are not configured.
PFC Mode	PFC configuration in DCB map: On (enabled) or Off.
PG	Priority group configured in the DCB map.
TSA	Transmission scheduling algorithm used by the priority group: Enhanced Transmission Selection (ETS).
BW	Percentage of bandwidth allocated to the priority group.
PFC	PFC setting for the priority group: On (enabled) or Off.
Priorities	802.1p priorities configured in the priority group.

Example

```
FTOS# show qos dcb-map dcbmap2

State   :Complete
PfcMode:ON
--------------------
```

```
PG:0 TSA:ETS  BW:50  PFC:OFF
Priorities:0 1 2 4 5 6 7


PG:1 TSA:ETS  BW:50  PFC:ON
Priorities:3
```

Related Commands

dcb-map — creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports.

show interfaces dcbx detail

Displays the DCBx configuration on an Ethernet interface.

S5000

Syntax

`show interfaces type slot/port dcbx detail`

Parameters

interfaces *type slot/port*	Enter the `interfaces` keyword followed by the Ethernet interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To clear DCBx frame counters, use the `clear dcbx counters interface stack-unit/port` command.

The following table describes the `show interface dcbx detail` command output shown in the Example below.

Table 1. Output Fields for the `show interface dcbx detail` Command

Field	Description
Interface	Interface type with chassis slot and port number.
Port-Role	Indicates the configured DCBx port role: auto-upstream, auto-downstream, config-source, or manual.

Field	Description
DCBx Operational Status	Operational status (enabled or disabled) is used to elect a configuration source and internally propogate a DCB configuration. The DCBx operational status is a combination of PFC and ETS operational status.
Reason:	Displays when the DCBx operational status of a port is disabled (down). For a description of each reason, refer to the DCB chapter in the *S5000 Configuration Guide*.
Configuration Source	Specifies whether the port serves as the DCBx configuration source on the switch: true (yes) or false (no).
Local DCBx Compatibility mode	DCBx version accepted in a DCB configuration as compatible. In auto-upstream mode, a port can only receive a DCBx version supported on the remote peer.
Local DCBx Configured mode	DCBx version configured on the port: CEE, CIN, IEEE v2 .5, or Auto (port auto-configures to use the DCBx version received from a peer).
Peer Operating version	DCBx version that the peer uses to exchange DCB parameters.
Local DCBx TLVs Transmitted	Transmission status (enabled or disabled) of advertised DCB TLVs (see TLV code at the top of the show command output).
Local DCBx Status: DCBx Operational Version	DCBx version advertised in Control TLVs.
Local DCBx Status: DCBx Max Version Supported	Highest DCBx version supported in Control TLVs.
Local DCBx Status: Sequence Number	Sequence number transmitted in Control TLVs.
Local DCBx Status: Acknowledgment Number	Acknowledgement number transmitted in Control TLVs.
Local DCBx Status: Protocol State	Current operational state of the DCBx protocol: ACK or IN-SYNC.
Peer DCBx Status: DCBx Operational Version	DCBx version advertised in Control TLVs received from the peer device.
Peer DCBx Status: DCBx Max Version Supported	Highest DCBx version supported in Control TLVs received from the peer device.
Peer DCBx Status: Sequence Number	Sequence number transmitted in Control TLVs received from the peer device.

Field	Description
Peer TLV Statistics: Acknowledgment Number	Acknowledgement number transmitted in Control TLVs received from the peer device.
PFC TLV Statistics: Input PFC TLV pkts	Number of PFC TLVs received.
PFC TLV Statistics: Output PFC TLV pkts	Number of PFC TLVs transmitted.
PFC TLV Statistics: Error PFC pkts	Number of PFC error packets received.
PFC TLV Statistics: PFC Pause Tx pkts	Number of PFC pause frames transmitted.
PFC TLV Statistics: PFC Pause Rx pkts	Number of PFC pause frames received.
PG TLV Statistics: Input PG TLV Pkts	Number of PG TLVs received.
PG TLV Statistics: Output PG TLV Pkts	Number of PG TLVs transmitted.
PG TLV Statistics: Error PG TLV Pkts	Number of PG error packets received.
Application TLV Statistics: Input Appln Priority TLV pkts	Number of Application TLVs received.
Application TLV Statistics: Output Appln Priority TLV pkts	Number of Application TLVs transmitted.
Application TLV Statistics: Error Appln Priority TLV Pkts	Number of Application TLV error packets received.
Total DCBx Frames transmitted	Number of DCBx frames sent from the local port.
Total DCBx Frames received	Number of DCBx frames received from the remote peer port.
Total DCBx Frame errors	Number of DCBx frames with errors received.
Total DCBx Frames unrecognized	Number of unrecognizable DCBx frames received.

Example

```
FTOS(conf)# show interface tengigabitethernet 0/49 dcbx detail
FTOS#show interface te 0/49 dcbx detail

E-ETS Configuration TLV enabled
  e-ETS Configuration TLV disabled
R-ETS Recommendation TLV enabled
  r-ETS Recommendation TLV disabled
P-PFC Configuration TLV enabled
  p-PFC Configuration TLV disabled
F-Application priority for FCOE enabled
  f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled
  i-Application Priority for iSCSI disabled
-----------------------------------------------------------

Interface TenGigabitEthernet 0/49
  Remote Mac Address 00:00:00:00:00:11
   Port Role is Auto-Upstream
  DCBx Operational Status is Enabled
  Is Configuration Source? TRUE
```

```
Local DCBx Compatibility mode is CEE
  Local DCBx Configured mode is CEE
  Peer Operating version is CEE
  Local DCBx TLVs Transmitted: ErPfi

Local DCBx Status
-----------------
  DCBx Operational Version is 0
  DCBx Max Version Supported is 0
  Sequence Number: 2
  Acknowledgment Number: 2
  Protocol State: In-Sync

Peer DCBx Status:
----------------
  DCBx Operational Version is 0
  DCBx Max Version Supported is 255
  Sequence Number: 2
  Acknowledgment Number: 2
  2 Input PFC TLV pkts,3 Output PFC TLV pkts,0 Error PFC pkts,
0 PFC Pause Tx pkts  0 Pause Rx pkts
  2 Input PG TLV Pkts, 3 Output PG TLV Pkts, 0 Error PG TLV
Pkts
  2 Input Appln Priority TLV pkts, 0 Output Appln Priority TLV
pkts,
  0 Error Appln Priority TLV Pkts
  Total DCBx Frames transmitted 27
  Total DCBx Frames received 6
  Total DCBx Frame errors 0
  Total DCBx Frames unrecognized 0
```

show interfaces ets

Displays the ETS configuration applied to egress traffic on an Ethernet interface, including priority groups with priorities and bandwidth allocation.

S5000

Syntax

```
show interfaces type slot/port ets {summary | detail}
```

Parameters

***type slot/port* ets**	Enter the Ethernet interface type and slot/port or number information followed by the keyword `ets`. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
{summary | detail}	Enter the keyword `summary` for a summary list of results or enter the keyword `detail` for a full list of results.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To clear ETS TLV counters, use the `clear ets counters interface` *`port-type slot/port`* command.

The following table describes the fields displayed in `show interface ets` command output.

Table 2. Output Fields for the `show interface ets` Command

Field	Description
Interface	Interface type with stack-unit number and port number.
Max Supported TC Group	Maximum number of priority groups supported.
Number of Traffic Classes	Number of 802 .1p priorities currently configured.
Admin mode	ETS mode: on or off . When on, the scheduling and bandwidth allocation configured in an ETS output policy or received in a DCBx TLV from a peer can take effect on an interface.
Admin Parameters	ETS configuration on local port, including priority groups, assigned dot1p priorities, and bandwidth allocation.
Remote Parameters	ETS configuration on remote peer port, including admin mode (enabled if a valid TLV was received or disabled), priority groups, assigned dot1p priorities, and bandwidth allocation. If ETS admin mode is enabled on the remote port for DCBx exchange, the Willing bit received in ETS TLVs from the remote peer is included.
Local Parameters	ETS configuration on local port, including admin mode (enabled when a valid TLV is received from a peer), priority groups, assigned dot1p priorities, and bandwidth allocation.
Operational status (local port)	Port state for current operational ETS configuration: • `Init`: Local ETS configuration parameters were exchanged with the peer. • `Recommend`: Remote ETS configuration parameters were received from the peer. • `Internally propagated`: ETS configuration parameters were received from the configuration source.
ETS DCBx Oper status	DCBx operational status of the ETS configuration on the local port: up (match) or down (mismatch).
Reason:	Displays when DCBx operational status for ETS on a port is down. For a description of each reason, refer to the DCB chapter in the *S5000 Configuration Guide*.

Field	Description
State Machine Type	Type of state machine used for DCBx exchanges of ETS parameters: Feature — for legacy DCBx versions; Asymmetric — for an IEEE version.
Conf TLV Tx Status	Status of ETS Configuration TLV advertisements: enabled or disabled.
Reco TLV Tx Status	Status of ETS Recommendation TLV advertisements: enabled or disabled.
Input Conf TLV pkts	Number of ETS Configuration TLVs received.
Output Conf TLV pkts	Number of ETS Configuration TLVs transmitted.
Error Conf TLV pkts	Number of ETS Error Configuration TLVs received.

The following table describes the fields displayed in `show interface ets` command output.

Example (summary)

```
FTOS(conf)# show interfaces tengigabitethernet 0/0 ets summary
Interface TenGigabitEthernet 0/0
Max Supported TC Groups is 4
Number of Traffic Classes is 8
Admin mode is on
Admin Parameters :
------------------
Admin is enabled
TC-grp Priority#       Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
1                       0%        ETS
2                       0%        ETS
3                       0%        ETS
4                       0%        ETS
5                       0%        ETS
6                       0%        ETS
7                       0%        ETS

Priority#               Bandwidth TSA
0                       13%       ETS
1                       13%       ETS
2                       13%       ETS
3                       13%       ETS
4                       12%       ETS
5                       12%       ETS
6                       12%       ETS
7                       12%       ETS
Remote Parameters:
-------------------
Remote is disabled

Local Parameters :
------------------
Local is enabled
TC-grp Priority#       Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
1                       0%        ETS
2                       0%        ETS
3                       0%        ETS
4                       0%        ETS
5                       0%        ETS
6                       0%        ETS
```

```
7                       0%        ETS

Priority#               Bandwidth TSA
0                       13%       ETS
1                       13%       ETS
2                       13%       ETS
3                       13%       ETS
4                       12%       ETS
5                       12%       ETS
6                       12%       ETS
7                       12%       ETS
Oper status is init
ETS DCBx Oper status is Down
Reason: Port shutdown
State Machine Type is Asymmetric
Conf TLV Tx Status is enabled
Reco TLV Tx Status is enabled
```

Example (detail)

```
FTOS(conf)# show interfaces tengigabitethernet 0/0 ets detail
Interface TenGigabitEthernet 0/0
Max Supported TC Groups is 4
Number of Traffic Classes is 8
Admin mode is onAdmin Parameters :
------------------
Admin is enabled
TC-grp  Priority#         Bandwidth  TSA
0       0,1,2,3,4,5,6,7   100%       ETS
1                         0%         ETS
2                         0%         ETS
3                         0%         ETS
4                         0%         ETS
5                         0%         ETS
6                         0%         ETS
7                         0%         ETS

Priority#  Bandwidth  TSA
0          13%        ETS
1          13%        ETS
2          13%        ETS
3          13%        ETS
4          12%        ETS
5          12%        ETS
6          12%        ETS
7          12%        ETS

Remote Parameters:
-------------------
Remote is disabled

Local Parameters :
------------------
Local is enabled
TC-grp Priority#        Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
1                       0%        ETS
2                       0%        ETS
3                       0%        ETS
4                       0%        ETS
5                       0%        ETS
6                       0%        ETS
7                       0%        ETS

Priority#               Bandwidth TSA
```

```
0                       13%       ETS
1                       13%       ETS
2                       13%       ETS
3                       13%       ETS
4                       12%       ETS
5                       12%       ETS
6                       12%       ETS
7                       12%       ETS

Oper status is init
Conf TLV Tx Status is disabled
ETS DCBx Oper status is Down
Reason: Port shutdown
State Machine Type is Feature

0 Input Conf TLV Pkts, 0 Output Conf TLV Pkts, 0 Error Conf
TLV Pkts
```

show interfaces pfc

Displays the PFC configuration applied to ingress traffic on an Ethernet interface, including priorities and link delay.

S5000

Syntax

`show interfaces type slot/port pfc {summary | detail}`

Parameters

***type slot/ port* pfc**	Enter the Ethernet interface type and slot/port or number information followed by the keyword `pfc`. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
{summary | detail}	Enter the keyword `summary` for a summary list of results or enter the keyword `detail` for a full list of results.

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To clear the PFC TLV counters, use the `clear pfc counters interface port-type slot/port` command.

The following table describes the `show interface pfc {summary}` command output shown in the Example below.

Table 3. Output Fields for the `show interface pfc` Command

Field	Description
Interface	Interface type with stack-unit number and port number.
Admin mode is on Admin is enabled	PFC admin mode is on or off with a list of the configured PFC priorities . When the PFC admin mode is on, PFC advertisements are enabled to be sent and received from peers; received PFC configuration will take effect. The admin operational status for a DCBx exchange of PFC configuration is enabled or disabled.
Remote is enabled, Priority list Remote Willing Status is enabled	Operational status (enabled or disabled) of peer device for DCBx exchange of PFC configuration with a list of the configured PFC priorities . Willing status of peer device for DCBx exchange (Willing bit received in PFC TLV): enabled or disable.
Local is enabled	DCBx operational status (enabled or disabled) with a list of the configured PFC priorities.
Operational status (local port)	Port state for current operational PFC configuration: • `Init`: Local PFC configuration parameters were exchanged with the peer. • `Recommend`: Remote PFC configuration parameters were received from the peer. • `Internally propagated`: PFC configuration parameters were received from the configuration source.
PFC DCBx Oper status	DCBx operational status of the exchange of PFC configuration on the local port: up (match) or down (mismatch).
Reason:	Displays when the DCBx operational status for PFC on a port is down. For a description of each reason, refer to the DCB chapter in the S5000 Configuration Guide.
State Machine Type	Type of state machine used for DCBx exchanges of the PFC parameters: Feature — for legacy DCBx versions; Symmetric — for an IEEE version.
TLV Tx Status	Status of the PFC TLV advertisements: enabled or disabled.

Field	Description
PFC Link Delay	Link delay (in quanta) used to pause specified priority traffic.
Application Priority TLV: FCOE TLV Tx Status	Status of FCoE advertisements in application priority TLVs from the local DCBx port: enabled or disabled.
Application Priority TLV: iSCSI TLV Tx Status	Status of iSCSI advertisements in application priority TLVs from the local DCBx port: enabled or disabled.
Application Priority TLV: Local FCOE Priority Map	Priority bitmap the local DCBx port uses in FCoE advertisements in application priority TLVs.
Application Priority TLV: Local iSCSI Priority Map	Priority bitmap the local DCBx port uses in iSCSI advertisements in application priority TLVs.
Application Priority TLV: Remote FCOE Priority Map	Status of FCoE advertisements in application priority TLVs from the remote peer port: enabled or disabled.
Application Priority TLV: Remote iSCSI Priority Map	Status of iSCSI advertisements in application priority TLVs from the remote peer port: enabled or disabled.
Input TLV pkts	Number of PFC TLVs received.
Output TLV pkts	Number of PFC TLVs transmitted.
Error TLV pkts	Number of PFC error packets received.
Pause Tx pkts	Number of PFC pause frames transmitted.
Pause Rx pkts	Number of PFC pause frames received.
Input Appln Priority TLV pkts	Number of Application Priority TLVs received.
Output Appln Priority TLV pkts	Number of Application Priority TLVs transmitted.
Error Appln Priority TLV pkts	Number of Application Priority error packets received.

Example

```
FTOS# show interfaces tengigabitethernet 0/49 pfc summary
Interface TenGigabitEthernet 0/49
  Admin mode is on
  Admin is enabled
  Remote is enabled, Priority list is 4
  Remote Willing Status is enabled
  Local is enabled
  Oper status is Recommended
  PFC DCBx Oper status is Up
  State Machine Type is Feature
  TLV Tx Status is enabled
  PFC Link Delay 45556 pause quantams
  Application Priority TLV Parameters :
```

```
  -------------------------------------
  FCOE TLV Tx Status is disabled
  ISCSI TLV Tx Status is disabled
  Local FCOE PriorityMap is 0x8
  Local ISCSI PriorityMap is 0x10
  Remote FCOE PriorityMap is 0x8
  Remote ISCSI PriorityMap is 0x8

FTOS# show interfaces tengigabitethernet 0/49 pfc detail
  Interface TenGigabitEthernet 0/49
  Admin mode is on
  Admin is enabled
  Remote is enabled
  Remote Willing Status is enabled
  Local is enabled
  Oper status is recommended
  PFC DCBx Oper status is Up
  State Machine Type is Feature
  TLV Tx Status is enabled
  PFC Link Delay 45556 pause quanta
  Application Priority TLV Parameters :
  -------------------------------------
  FCOE TLV Tx Status is disabled
  ISCSI TLV Tx Status is disabled
  Local FCOE PriorityMap is 0x8
  Local ISCSI PriorityMap is 0x10
  Remote FCOE PriorityMap is 0x8
  Remote ISCSI PriorityMap is 0x8
  0 Input TLV pkts, 1 Output TLV pkts, 0 Error pkts,
  0 Pause Tx pkts, 0 Pause Rx pkts
  0 Input Appln Priority TLV pkts, 1 Output Appln Priority TLV
pkts,
  0 Error Appln Priority TLV Pkts
```

show interfaces pfc statistics

Displays counters for the PFC frames received and transmitted (by dot1p priority class) on an interface.

S5000

Syntax `show interfaces` *`type slot/port`* `pfc statistics`

Parameters

***type slot/port* pfc statistics**	Enter the interface type and slot/port or number information followed by the keywords `pfc statistics`. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (Summary)

```
FTOS#show interfaces te 0/0 pfc statistics

Interface TenGigabitEthernet 0/0

Priority  Rx XOFF Frames Rx Total Frames Tx Total Frames
-------------------------------------------------------
0         0              0               0
1         0              0               0
2         0              0               0
3         0              0               0
4         0              0               0
5         0              0               0
6         0              0               0
7         0              0               0
```

show stack-unit stack-ports ets detail

Displays the ETS configuration applied to egress traffic on stacked ports, including the ETS operational mode on each unit and the configured priority groups with dot1p priorities, bandwidth allocation, and scheduler type.

S5000

Syntax

```
show stack-unit {unit-number | all} stack-ports {all ets detail
```

Parameters

stack-unit *unit-number*	Enter the keyword `stack-unit` followed by a number. The range is 0 to 11.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (Summary)

```
FTOS(conf)# show stack-unit all stack-ports all ets detail

Stack unit 0 stack port all
Max Supported TC Groups is 4
Number of Traffic Classes is 1
Admin mode is on

Admin Parameters:
--------------------
Admin is enabled
TC-grp Priority#        Bandwidth TSA
------------------------------------------------
0      0,1,2,3,4,5,6,7  100%      ETS
1                       -         -
2                       -         -
3                       -         -
4                       -         -
```

```
5                       -        -
6                       -        -
7                       -        -
8                       -        -

Stack unit 1 stack port all
Max Supported TC Groups is 4
Number of Traffic Classes is 1
Admin mode is on
Admin Parameters:
--------------------
Admin is enabled
TC-grp Priority#        Bandwidth TSA
------------------------------------------------
0      0,1,2,3,4,5,6,7  100%      ETS
1                       -         -
2                       -         -
3                       -         -
4                       -         -
5                       -         -
6                       -         -
7                       -         -
8                       -         -
```

show stack-unit stack-ports pfc detail

Displays the PFC configuration applied to ingress traffic on stacked ports, including PFC Operational mode on each unit with the configured priorities, link delay, and number of pause packets sent and received.

S5000

Syntax `show stack-unit {unit-number | all } stack-ports all pfc detail`

Parameters

stack-unit *unit-number*	Enter the keyword `stack-unit` followed by a number. The range is 0 to 11.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information To clear the PFC TLV counters, use the `clear pfc counters stack-unit { unit-id | all } stack-ports all` command.

Example (Summary)

```
FTOS(conf)# show stack-unit all stack-ports all pfc detail

stack unit 0 stack-port all
  Admin mode is On
  Admin is enabled, Priority list is 4-5
  Local is enabled, Priority list is 4-5
  Link Delay 45556 pause quantum
  0 Pause Tx pkts, 0 Pause Rx pkts

stack unit 1 stack-port all
  Admin mode is On
Admin is enabled, Priority list is 4-5
Local is enabled, Priority list is 4-5
Link Delay 45556 pause quantum
0 Pause Tx pkts, 0 Pause Rx pkts
```

15

Dynamic Host Configuration Protocol (DHCP)

Dynamic host configuration protocol (DHCP) is an application layer protocol that dynamically assigns IP addresses and other configuration parameters to network end-stations (hosts) based on configuration policies determined by network administrators.

The basic DHCP commands are supported by FTOS on the S5000 switch.

This chapter contains the following sections:

- Commands to Configure the System to be a DHCP Server
- Commands to Configure Secure DHCP

Commands to Configure the System to be a DHCP Server

Use the following commands to configure the system to ba DHCP server.

clear ip dhcp

Reset the DHCP counters.

S5000

Syntax

```
clear ip dhcp [binding {address} | conflict | server
statistics]
```

Parameters

binding	Enter the keyword `binding` to delete all entries in the binding table.
address	Enter the IP address to clear the binding entry for a single IP address.
conflicts	Enter the keyword `conflicts` to delete all of the log entries created for IP address conflicts.
server statistics	Enter the keywords `server statistics` to clear all the server counter information.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	Entering <CR> after the `clear ip dhcp binding` command clears all the IPs from the binding table.

debug ip dhcp server

Display FTOS debugging messages for DHCP.

S5000

Syntax

```
debug ip dhcp server [events | packets]
```

Parameters

events	Enter the keyword `events` to display the DHCP state changes.
packet	Enter the keyword `packet` to display packet transmission/reception.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

default-router

Assign a default gateway to clients based on the address pool.

S5000

Syntax

```
default-router address [address2...address8]
```

Parameters

address	Enter a list of routers that may be the default gateway for clients on the subnet. You may specify up to eight routers. List them in order of preference.

Defaults none

Command Modes DHCP <POOL>

Command History

Version 9.0(1.3)	Introduced on the S5000.

disable

Disable the DHCP server.

S5000

Syntax	`disable` DHCP Server is disabled by default. Enable the system to be a DHCP server using the `no disable` command.	
Defaults	Disabled	
Command Modes	CONFIGURATION	
Command History	**Version 9.0(1.3)**	Introduced on the S5000.

dns-server

Assign a DNS server to clients based on address pool.

S5000

Syntax	`dns-server address [address2...address8]`	
Parameters	***address***	Enter the a list of DNS servers that may service clients on the subnet. You may list up to eight servers, in order of preference.
Defaults	none	
Command Modes	DHCP <POOL>	
Command History	**Version 9.0(1.3)**	Introduced on the S5000.

domain-name

Assign a domain to clients based on the address pool.

S5000

Syntax	`domain-name` *`name`*	
Parameters	***name***	Give a name to the group of addresses in a pool.

Defaults	none
Command Modes	DHCP <POOL>
Command History	**Version 9.0(1.3)** Introduced on the S5000.

excluded-address

Prevent the server from leasing an address or range of addresses in the pool.

S5000

Syntax `excluded-address [address | low-address high-address]`

Parameters

address	Enter a single address to be excluded from the pool.
low-address	Enter the lowest address in a range of addresses to be excluded from the pool.
high-address	Enter the highest address in a range of addresses to be excluded from the pool.

Defaults	none
Command Modes	DHCP
Command History	**Version 9.0(1.3)** Introduced on the S5000.

hardware-address

For manual configurations, specify the client hardware address.

S5000

Syntax `hardware-address address`

Parameters

address	Enter the hardware address of the client.

Defaults	none
Command Modes	DHCP <POOL>
Command History	**Version 9.0(1.3)** Introduced on the S5000.

host

For manual (rather than automatic) configurations, assign a host to a single-address pool.

S5000

Syntax	`host address`
Parameters	

address/mask	Enter the host IP address and subnet mask.

Defaults	none
Command Modes	DHCP <POOL>
Command History	

Version 9.0(1.3)	Introduced on the S5000.

lease

Specify a lease time for the addresses in a pool.

S5000

Syntax	`lease {days [hours] [minutes] | infinite}`
Parameters	

days	Enter the number of days of the lease. The range is 0 to 31.
hours	Enter the number of hours of the lease. The range is 0 to 23.
minutes	Enter the number of minutes of the lease. The range is 0 to 59.
infinite	Specify that the lease never expires.

Defaults	**24 hours**
Command Modes	DHCP <POOL>
Command History	

Version 9.0(1.3)	Introduced on the S5000.

netbios-name-server

Specify the NetBIOS Windows Internet Naming Service (WINS) name servers, in order of preference, that are available to Microsoft Dynamic Host Configuration Protocol (DHCP) clients.

S5000

Syntax `netbios-name-server address [address2...address8]`

Parameters

address	Enter the address of the NETBIOS name server. You may enter up to eight, in order of preference.

Defaults none

Command Modes DHCP <POOL>

Command History

Version 9.0(1.3)	Introduced on the S5000.

netbios-node-type

Specify the NetBIOS node type for a Microsoft DHCP client. Dell Networking recommends specifying clients as `hybrid`.

S5000

Syntax `netbios-node-type type`

Parameters

type	Enter the NETBIOS node type: • Broadcast: Enter the keyword `b-node`. • Hybrid: Enter the keyword `h-node`. • Mixed: Enter the keyword `m-node`. • Peer-to-peer: Enter the keyword `p-node`.

Defaults **Hybrid**

Command Modes DHCP <POOL>

Command History

Version 9.0(1.3)	Introduced on the S5000.

network

Specify the range of addresses in an address pool.

S5000

Syntax	`network` *`network /prefix-length`*
Parameters	
network/ prefix-length	Specify a range of addresses. Prefix-length range is 17 to 31.
Defaults	none
Command Modes	DHCP <POOL>
Command History	
Version 9.0(1.3)	Introduced on the S5000.

pool

Create an address pool.

S5000

Syntax	`pool` *`name`*
Parameters	
name	Enter the address pool’s identifying name.
Defaults	none
Command Modes	DHCP
Command History	
Version 9.0(1.3)	Introduced on the S5000.

show ip dhcp binding

Display the DHCP binding table.

S5000

Syntax	`show ip dhcp binding`
Defaults	none

Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

show ip dhcp configuration

Display the DHCP configuration.

S5000

Syntax `show ip dhcp configuration [global | pool name]`

Parameters

pool *name*	Display the configuration for a DHCP pool.
global	Display the DHCP configuration for the entire system.

Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

show ip dhcp conflict

Display the address conflict log.

S5000

Syntax `show ip dhcp conflict address`

Parameters

address	Display a particular conflict log entry.

Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

show ip dhcp server

Display the DHCP server statistics.

S5000

Syntax	`show ip dhcp server statistics`
Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Commands to Configure Secure DHCP

DHCP, as defined by RFC 2131, provides no authentication or security mechanisms. Secure DHCP is a suite of features that protects networks that use dynamic address allocation from spoofing and attacks.

arp inspection

Enable dynamic arp inspection (DAI) on a VLAN.

S5000

Syntax	`arp inspection`
Defaults	Disabled
Command Modes	INTERFACE VLAN
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	arp inspection-trust – specifies a port as trusted so that ARP frames are not validated against the binding table.

arp inspection-trust

Specify a port as trusted so that ARP frames are not validated against the binding table.

S5000

Syntax

```
arp inspection-trust
```

Defaults

Disabled

Command Modes

- INTERFACE
- INTERFACE PORT-CHANNEL

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

arp inspection – enables dynamic ARP inspection on a VLAN.

clear ip dhcp snooping

Clear the DHCP binding table.

S5000

Syntax

```
clear ip dhcp snooping binding
```

Defaults

none

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

show ip dhcp snooping – displays the contents of the DHCP binding table.

ip dhcp relay

Enable Option 82.

S5000

Syntax

```
ip dhcp relay information-option [remote-id | trust-downstream]
```

Parameters

remote-id	Configure the system to enable the remote-id string in option-82.
trust-downstream	Configure the system to trust Option 82 when it is received from the previous-hop router.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip dhcp snooping

Enable DHCP snooping globally.

S5000

Syntax `[no] ip dhcp snooping`

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When enabled, no learning takes place until you enable snooping on a VLAN. After disabling DHCP snooping, the binding table deletes and Option 82, IP Source Guard, and Dynamic ARP Inspection are disabled.

You do not have to enable relay agent to snoop on Layer 2 interfaces.

Related Commands

ip dhcp snooping vlan – enables DHCP snooping on one or more VLANs.

ip dhcp snooping binding

Create a static entry in the DHCP binding table.

S5000

Syntax `[no] ip dhcp snooping binding mac address vlan-id vlan-id ip ip-address interface type slot/port lease number`

Parameters

mac *address*	Enter the keyword `mac` followed by the MAC address of the host to which the server is leasing the IP address.

vlan-id *vlan-id*	Enter the keywords `vlan-id` followed by the VLAN to which the host belongs. The range is 2 to 4094.
ip *ip-address*	Enter the keyword `ip` followed by the IP address that the server is leasing.
interface *type*	Enter the keyword `interface` followed by the type of interface to which the host is connected: • For a Gigabit Ethernet interface, enter the keyword `gigabitethernet`. • For a Ten Gigabit Ethernet interface, enter the keyword `tengigabitethernet`. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`.
slot/port	Enter the slot and port number of the interface.
lease *time*	Enter the keyword `lease` followed by the amount of time the IP address will be leased. The range is 1 to 4294967295.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands show ip dhcp snooping – displays the contents of the DHCP binding table.

ip dhcp snooping database

Delay writing the binding table for a specified time.

S5000

Syntax `ip dhcp snooping database write-delay` *`minutes`*

Parameters

minutes	The range is 5 to 21600.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip dhcp snooping database renew

Renew the binding table.

S5000

Syntax	`ip dhcp snooping database renew`
Defaults	none
Command Modes	• EXEC • EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ip dhcp snooping trust

Configure an interface as trusted.

S5000

Syntax	`[no] ip dhcp snooping trust`
Defaults	**Untrusted**
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ip dhcp source-address-validation

Enable the IP Source Guard.

S5000

Syntax	`[no] ip dhcp source-address-validation [ipmac]`
Parameters	**ipmac** Enable IP+MAC Source Address Validation.
Defaults	Disabled
Command Modes	INTERFACE

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must allocate at least one FP block to `ipmacacl` before you can enable IP+MAC Source Address Validation.

1. Use the `cam-acl l2acl` command from CONFIGURATION mode.
2. Save the running-config to the startup-config.
3. Reload the system.

ip dhcp snooping vlan

Enable DHCP Snooping on one or more VLANs.

S5000

Syntax

```
[no] ip dhcp snooping vlan name
```

Parameters

name	Enter the name of a VLAN on which to enable DHCP Snooping.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When enabled, the system begins creating entries in the binding table for the specified VLAN(s).

NOTE: Learning only happens if there is a trusted port in the VLAN.

Related Commands

ip dhcp snooping trust – configures an interface as trusted.

ip dhcp snooping verify mac-address

Validate a DHCP packet’s source hardware address against the client hardware address field (CHADDR) in the payload.

S5000

Syntax

```
[no] ip dhcp snooping verify mac-address
```

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip dhcp snooping

Display the contents of the DHCP binding table or display the interfaces configured with IP Source Guard.

S5000

Syntax `show ip dhcp snooping [binding | source-address-validation]`

Parameters

binding	Display the interfaces configured with IP Source Guard.
source-address-validation	Display the interfaces configured with IP Source Guard.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands clear ip dhcp snooping – clears the contents of the DHCP binding table.

16

Equal Cost Multi-Path Overview (ECMP)

ECMP is supported on the S5000 switch.

ecmp-group

Provides a mechanism to monitor traffic distribution on an ECMP link bundle. A system log is generated when the standard deviation of traffic distribution on a member link exceeds a defined threshold.

S5000

Syntax

`ecmp-group` *`ecmp-group-id`*

To remove the selected interface, use the `ecmp-group no interface` command.

To disable link bundle monitoring, use the `ecmp-group no link-bundle-monitor` command.

Parameters

ecmp-group-id	Enter the number of the ECMP group. The range is 1 to 64.
interface*type* *slot/port*	Enter the following keywords and slot/port to add the interface to the ECMP group: • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

Defaults

Off

Command Modes

- CONFIGURATION
- CONFIGURATION ECMP-GROUP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	Using CONFIGURATION mode, create an ECMP group ID. You can then assign interfaces to the ECMP group using CONFIGURATION ECMP-GROUP mode. You can also enable on the port-channel configuration using the CONFIGURATION ECMP-GROUP command mode.

hash-algorithm

Changes the hash algorithm used to distribute traffic flows across a Port Channel.

S5000

Syntax

`hash-algorithm [`*`algorithm-number`*`] | [ecmp {crc | crc-upper | xor | dest-ip | lsb] | [lag {crc | xor} | [seed]`

To return to the default hash algorithm, use the `no hash-algorithm` command.

To return to the default Equal-cost Multipath Routing (ECMP) hash algorithm, use the `no hash-algorithm ecmp` *algorithm-value* command.

Parameters

algorithm-number	Enter the algorithm number. The range is 0 to 47.
ecmp	(OPTIONAL) Enter the `ecmp` keyword followed by the `crc`, `crc-upper`, `xor`, `dest-ip`, or `lsb` keywords to specify the metric on which to base route calculations for load balancing.
lag	(OPTIONAL) Enter the `lag` keyword followed by the `crc` or `xor` keywords to specify routing metrics for a specific port-channel.
seed	Enter a value with which to seed the algorithm. The range is 0 to 2147483646.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The different hash algorithms are based on the number of Port Channel members and packet values. The default hash algorithm (number 0) yields the most balanced results in various test scenarios, but if the default algorithm does not provide a satisfactory distribution of traffic, use the hash-algorithm command to designate another algorithm.

When a Port Channel member leaves or is added to the Port Channel, the hash algorithm is recalculated to balance traffic across the members.

hash-algorithm ecmp

Change the hash algorithm used to distribute traffic flows across an ECMP (equal-cost multipath routing) group.

S5000

Syntax

```
hash-algorithm ecmp {crc-upper} | {crc} | {dest-ip} | {lsb} |
{xor}
```

To return to the default hash algorithm, use the `no hash-algorithm ecmp` command.

Parameters

crc	Uses specified polynomicals or bits of computed cyclic redundancy checks (CRC) for the hash computation.
crc-upper	Uses the upper 32 bits of the key for the hash computation.
dest-ip	Uses the destination IP for ECMP hashing.
lsb	Returns the LSB of the key as the hash.
xor	Uses the lower 8 bits of the key for the hash computation.

Defaults

- crc-lower
- dest-ip enabled

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The hash value calculated with the hash-algorithm command is unique to the entire chassis. The default ECMP hash configuration is **crc-lower**. This takes the lower 32 bits of the hash key to compute the egress port and is the “fall-back” configuration if you have not configured anything else.

The different hash algorithms are based on the number of ECMP group members and packet values. The default hash algorithm yields the most balanced results in various test scenarios, but if the default algorithm does not provide satisfactory distribution of traffic, use this command to designate another algorithm.

When a member leaves or is added to the ECMP group, the hash algorithm is recalculated to balance traffic across the members.

Related Commands load balance

ip ecmp-group

Enable and specify the maximum number of ecmp that the L3 CAM hold for a route, By default, when maximum paths are not configured, the CAM can hold a maximum of 16 ecmp per route.

S5000

Syntax

`ip ecmp-group {maximum-paths | {number} {path-fallback}`

To negate a command, use the `no ip ecmp-group maximum-paths {number}` command.

Parameters

maximum-paths	Specify the maximum number of ECMP for a route. The range is 2 to 64.
path-fallback	Use the keyword `path-fallback` to enable this feature. If you enable the feature, re-enter this keyword to disable the feature.

Defaults 16

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information You must save the new ECMP settings to the startup-config (`write-mem`) then reload the system for the new settings to take effect.

Related Commands show ip cam stack-unit – Display content-addressable memory (CAM) entries for an S5000 switch.

link-bundle-distribution trigger-threshold

Provides a mechanism to set the threshold to trigger when traffic distribution will begin being monitored on an ECMP link bundle.

S5000

Syntax `link-bundle-distribution trigger-threshold [percent]`

Parameters

percent	Indicate the threshold value when traffic distribution will start being monitored on an ECMP link bundle. The range is 1 to 90%. The default is 60%.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

link-bundle-monitor enable

Provides a mechanism to enable monitoring of traffic distribution on an ECMP link bundle.

S5000

Syntax	`link-bundle-monitor enable` To exit from ecmp group mode, use the `exit` command.
Command Modes	• ECMP-GROUP • PORT-CHANNEL INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

17

FCoE Transit

Use FTOS commands to enable the FCoE Transit feature and configure FIP snooping on the S5000 switch on Ethernet interfaces. When you enable an S5000 for FCoE transit, the switch functions as a FIP snooping bridge.

In a converged Ethernet network, an S5000 switch can operate as an intermediate Ethernet bridge to snoop on Fibre Channel over Ethernet initialization protocol (FIP) packets during the login process on Fibre Channel over Ethernet (FCoE) forwarders (FCFs). Acting as a transit FIP snooping bridge, the switch uses dynamically created access control lists (ACLs) to permit only authorized FCoE traffic to transmit between an FCoE end-device and an FCF.

clear fip-snooping database interface vlan

Clear FIP snooping information on a VLAN for a specified FCoE MAC address, ENode MAC address, or FCF MAC address, and remove the corresponding ACLs generated by FIP snooping.

S5000

Syntax

```
clear fip-snooping database interface vlan {vlan-id} enode
{enode-mac-address} | fcf {fcf-mac-address} | session {session-
mac-address}
```

Parameters

enode-mac-address	Enter the ENode MAC address to be cleared of FIP snooping information.
fcf-mac-address	Enter the FCF MAC address to be cleared of FIP snooping information.
session-mac-address	Enter the MAC address for the session to be cleared of FIP snooping information.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear fip-snooping statistics

Clears the statistics on the FIP packets snooped on all VLANs, a specified VLAN, or a specified port interface.

S5000

Syntax

```
clear fip-snooping statistics [interface vlan vlan-id |
interface port-type port/slot | interface port-channel port-
channel-number]
```

Parameters

vlan-id	Enter the VLAN ID of the FIP packet statistics to be cleared.
port-type port/slot	Enter the port-type and slot number of the FIP packet statistics to be cleared.
port-channelnumber	Enter the port channel number of the FIP packet statistics to be cleared.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug fip snooping

Enable debugging on FIP snooping.

S5000

Syntax

```
debug fip-snooping [all | acl | error | ifm | info | ipc | rx |
stacking | tx]
```

Parameters

all	Enter the keyword `all` to enable debugging on all the options.
acl	Enter the keyword `acl`
error	Enter the keyword `error`
ifm	Enter the keyword `ifm`
info	Enter the keyword `info`
ipc	Enter the keyword `ipc`
rx	Enter the keyword `rx`
stacking	Enter the keyword `stacking`
tx	Enter the keyword `tx`

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

feature fip-snooping

Enable the S5000 for FCoE transit and FIP snooping.

S5000

Syntax

```
feature fip-snooping
```

To disable the FCoE transit feature, use the `no feature fip-snooping` command.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

fip-snooping enable

Enable FIP snooping on all VLANs or on a specified VLAN.

S5000

Syntax

```
fip-snooping enable
```

To disable FIP snooping on all or a specified VLAN, use the `no fip-snooping enable` command.

Defaults FIP snooping is disabled on all VLANs.

Command Modes

- CONFIGURATION
- VLAN INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The maximum number of FCoE VLANs supported on the switch is eight.

fip-snooping fc-map

Configure the FC-MAP value FIP snooping uses on all VLANs.

S5000

Syntax	`fip-snooping fc-map` *`fc-map-value`* To remove the configured FM-MAP value, use the `no fip-snooping fc-map` command.
Parameters	*fc-map-value* — Enter the FC-MAP value FIP snooping uses. The range is 0EFC00 to 0EFCFF.
Defaults	0x0EFC00
Command Modes	• CONFIGURATION • VLAN INTERFACE
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

fip-snooping max-sessions-per-enodemac

Configure the maximum number of FIP-snooping sessions supported on the switch for an ENode MAC address.

S5000

Syntax	`fip-snooping max-sessions-per-enodemac` *`max-value`* To remove the configured number of supported sessions, use the `no fip-snooping max —sessions-per-enodemac` command.
Parameters	*max-value* — Enter the maximum number of FIP snooping sessions with an ENode that are supported on the switch. The range is 1 to 64.
Defaults	32
Command Modes	• CONFIGURATION
Command History	**Version 9.0(1.3)** — Introduced on the S5000.
Usage Information	The maximum number of supported FIP snooping sessions that you configure is displayed in the running configuration (if it is not the default value) and in `show fip-snooping config` output. If you configure a smaller number of supported sessions than was previously configured, all current FIP snooping sessions continue and a warning message is displayed. If a greater

number of sessions are active with an ENode, additional sessions are not allowed as long as the total number is greater than the newly configured limit.

When the maximum number of FIP snooping sessions for an ENode are already active on the switch, a log message is recorded if the ENode tries to log in to initiate another session.

fip-snooping port-mode fcf

Configure the port for bridge-to-FCF links.

S5000

Syntax

```
fip-snooping port-mode fcf
```

To disable the bridge-to-FCF link on a port, use the `no fip-snooping port-mode fcf` command.

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The maximum number of FCFs supported per FIP snooping-enabled VLAN is four.

NOTE: The FCoE-Trusted Port mode used to connect to another FIP snooping bridge (bridge-bridge link) is not supported on the S5000.

show fip-snooping config

Display the FIP snooping status and configured FC-MAP values.

S5000

Syntax

```
show fip-snooping config
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS# show fip-snooping config
FIP Snooping Feature enabled Status: Enabled
FIP Snooping Global enabled Status: Enabled
Global FC-MAP Value: 0X0EFC00

FIP Snooping enabled VLANs
VLAN   Enabled   FC-MAP
```

```
----    -------    --------
100     TRUE       0X0EFC00
```

show fip-snooping enode

Display information on the ENodes in FIP-snooped sessions, including the ENode interface and MAC address, FCF MAC address, VLAN ID and FC-ID.

S5000

Syntax

```
show fip-snooping enode [enode-mac-address]
```

Parameters

enode-mac-address	Enter the MAC address of the ENodes to be displayed.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show fip-snooping enode` command shown in the Example below.

Field	Description
ENode MAC	MAC address of the ENode.
ENode Interface	Slot/ port number of the interface connected to the ENode.
FCF MAC	MAC address of the FCF.
VLAN	VLAN ID number the session uses.
FC-ID	Fibre Channel session ID the FCF assigns.

Example

```
FTOS# show fip-snooping enode
Enode MAC         Enode Interface FCF MAC           VLAN FC-ID
--------- --------------- ------- ---- -----
d4:ae:52:1b:e3:cd Te 0/11         54:7f:ee:37:34:40 100
62:00:11
```

show fip-snooping fcf

Display information on the FCFs in FIP-snooped sessions, including the FCF interface and MAC address, FCF interface, VLAN ID, FC-MAP value, FKA advertisement period, and number of ENodes connected.

S5000

Syntax `show fip-snooping fcf [fcf-mac-address]`

Parameters

fcf-mac-address	Enter the MAC address of the FCF to be displayed.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The following describes the `show fip-snooping fcf` command shown in the Example below.

Field	**Description**
FCF MAC	MAC address of the FCF.
FCF Interface	Slot/port number of the interface to which the FCF is connected.
VLAN	VLAN ID number the session uses.
FC-MAP	FC-Map value the FCF advertises.
ENode Interface	Slot/ number of the interface connected to the ENode.
FKA_ADV_PERIOD	Time (in milliseconds) during which FIP keep-alive advertisements transmit.
No of ENodes	Number of ENodes connected to the FCF.
FC-ID	Fibre Channel session ID the FCF assigns.

Example

```
FTOS# show fip-snooping fcf
FCF MAC        FCF Interface VLAN FC-MAP FKA_ADV_PERIOD No. of
Enodes
------- ------------- ---- ------ -------------- -------------
54:7f:ee:37:34:40 Po 22      100 0e:fc:00 4000
2
```

show fip-snooping sessions

Display information on FIP-snooped sessions on all VLANs or a specified VLAN, including the ENode interface and MAC address, the FCF interface and MAC address, VLAN ID, FCoE MAC address and FCoE session ID number (FC-ID), worldwide node name (WWNN) and the worldwide port name (WWPN).

S5000

Syntax

`show fip-snooping sessions [interface vlan vlan-id]`

Parameters

vlan-id	Enter the vlan-id of the specified VLAN to be displayed.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show fip-snooping sessions` command shown in the Example below.

Field	Description
ENode MAC	MAC address of the ENode.
ENode Interface	Slot/ port number of the interface connected to the ENode.
FCF MAC	MAC address of the FCF.
FCF Interface	Slot/ port number of the interface to which the FCF is connected.
VLAN	VLAN ID number the session uses.
FCoE MAC	MAC address of the FCoE session the FCF assigns.
FC-ID	Fibre Channel ID the FCF assigns.
Port WWPN	Worldwide port name of the CNA port.
Port WWNN	Worldwide node name of the CNA port.

Example

```
FTOS# show fip-snooping sessions
Enode MAC Enode Intf FCF MAC FCF Intf VLAN FCoE MAC
 FC-ID Port WWPN
    Port WWNN
----------------------------------------------
00:00:c9:f1:e1:37 Te 0/28 54:7f:ee:34:77:4e Te 1/47 111
  0e:fc:00:b5:00:07 b5:00:07 10:00:00:00:c9:f1:e1:37
     20:00:00:00:c9:f1:e1:37
00:c0:dd:12:c0:05 Te 1/26 54:7f:ee:34:77:4e Te 1/47 111
  0e:fc:00:b5:00:75 b5:00:75 21:00:00:c0:dd:12:c0:05
    20:00:00:c0:dd:12:c0:05
```

show fip-snooping statistics

Display statistics on the FIP packets snooped on all interfaces, including VLANs, physical ports, and port channels.

S5000

Syntax

`show fip-snooping statistics [interface vlan` *`vlan-id`* `| interface` *`port-type port/slot`* `| interface port-channel` *`port-channel-number`*`]`

Parameters

vlan-id	Enter the VLAN ID of the FIP packet statistics displays.
port-type port/slot	Enter the port-type and slot number of the FIP packet statistics displays.
port-channel-number	Enter the port channel number of the FIP packet statistics displays.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following table describes the `show fip-snooping statistics` command output shown in the Example below.

Table 4. Output Fields for the **`show fip-snooping statistics`** Command

Field	Description
Number of VLAN Requests	Number of FIP-snooping VLAN request frames received on the interface.
Number of VLAN Notifications	Number of FIP-snooping VLAN notification frames received on the interface.
Number of Multicast Discovery Solicits	Number of FIP-snooping multicast discovery solicit frames received on the interface.
Number of Unicast Discovery Solicits	Number of FIP-snooping unicast discovery solicit frames received on the interface.
Number of FLOGI	Number of FIP-snooping FLOGI request frames received on the interface.
Number of FDISC	Number of FIP-snooping FDISC request frames received on the interface.
Number of FLOGO	Number of FIP-snooping FLOGO frames received on the interface.
Number of ENode Keep Alives	Number of FIP-snooping ENode keep-alive frames received on the interface.

Field	Description
Number of VN Port Keep Alives	Number of FIP-snooping VN port keep-alive frames received on the interface.
Number of Multicast Discovery Advertisements	Number of FIP-snooping multicast discovery advertisements received on the interface.
Number of Unicast Discovery Advertisements	Number of FIP-snooping unicast discovery advertisements received on the interface.
Number of FLOGI Accepts	Number of FIP FLOGI accept frames received on the interface.
Number of FLOGI Rejects	Number of FIP FLOGI reject frames received on the interface.
Number of FDISC Accepts	Number of FIP FDISC accept frames received on the interface.
Number of FDISC Rejects	Number of FIP FDISC reject frames received on the interface.
Number of FLOGO Accepts	Number of FIP FLOGO accept frames received on the interface.
Number of FLOGO Rejects	Number of FIP FLOGO reject frames received on the interface.
Number of CVLs	Number of FIP clear virtual link frames received on the interface.
Number of FCF Discovery Timeouts	Number of FCF discovery timeouts that occurred on the interface.
Number of VN Port Session Timeouts	Number of VN port session timeouts that occurred on the interface.
Number of Session failures due to Hardware Config	Number of session failures due to hardware configuration that occurred on the interface.

Example

```
FTOS# show fip-snooping statistics interface vlan 100
Number of Vlan Requests                :0
Number of Vlan Notifications           :0
Number of Multicast Discovery Solicits :2
Number of Unicast Discovery Solicits   :0
Number of FLOGI                        :2
Number of FDISC                        :16
Number of FLOGO                        :0
Number of Enode Keep Alive             :9021
Number of VN Port Keep Alive           :3349
Number of Multicast Discovery Advertisement :4437
Number of Unicast Discovery Advertisement :2
Number of FLOGI Accepts                :2
Number of FLOGI Rejects                :0
Number of FDISC Accepts                :16
Number of FDISC Rejects                :0
Number of FLOGO Accepts                :0
Number of FLOGO Rejects                :0
Number of CVL                          :0
Number of FCF Discovery Timeouts       :0
Number of VN Port Session Timeouts     :0
Number of Session failures due to Hardware Config :0
FTOS(conf)#

FTOS# show fip-snooping statistics int tengigabitethernet 0/11
Number of Vlan Requests                :1
Number of Vlan Notifications           :0
Number of Multicast Discovery Solicits :1
Number of Unicast Discovery Solicits   :0
Number of FLOGI                        :1
Number of FDISC                        :16
Number of FLOGO                        :0
Number of Enode Keep Alive             :4416
Number of VN Port Keep Alive           :3136
Number of Multicast Discovery Advertisement :0
Number of Unicast Discovery Advertisement :0
Number of FLOGI Accepts                :0
Number of FLOGI Rejects                :0
Number of FDISC Accepts                :0
Number of FDISC Rejects                :0
Number of FLOGO Accepts                :0
Number of FLOGO Rejects                :0
Number of CVL                          :0
Number of FCF Discovery Timeouts       :0
Number of VN Port Session Timeouts     :0
Number of Session failures due to Hardware Config :0
```

Example (Port Channel)

```
FTOS# show fip-snooping statistics interface port-channel 22
Number of Vlan Requests                :0
Number of Vlan Notifications           :2
Number of Multicast Discovery Solicits :0
Number of Unicast Discovery Solicits   :0
Number of FLOGI                        :0
Number of FDISC                        :0
Number of FLOGO                        :0
Number of Enode Keep Alive             :0
Number of VN Port Keep Alive           :0
Number of Multicast Discovery Advertisement :4451
Number of Unicast Discovery Advertisement :2
Number of FLOGI Accepts                :2
Number of FLOGI Rejects                :0
Number of FDISC Accepts                :16
Number of FDISC Rejects                :0
Number of FLOGO Accepts                :0
Number of FLOGO Rejects                :0
Number of CVL                          :0
Number of FCF Discovery Timeouts       :0
Number of VN Port Session Timeouts     :0
Number of Session failures due to Hardware Config :0
```

show fip-snooping system

Display information on the status of FIP snooping on the switch (enabled or disabled), including the number of FCoE VLANs, FCFs, ENodes, and currently active sessions.

S5000

Syntax `show fip-snooping system`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS# show fip-snooping system
Global Mode : Enabled
FCOE VLAN List (Operational) : 1, 100
FCFs                         : 1
Enodes                       : 2
Sessions                     : 17
```

show fip-snooping vlan

Display information on the FCoE VLANs on which FIP snooping is enabled.

S5000

Syntax `show fip-snooping vlan`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS# show fip-snooping vlan
* = Default VLAN
VLAN FC-MAP    FCFs Enodes Sessions
---- ------ ---- ------ --------
*1    -        -    -      -
100   0X0EFC00 1    2      17
```

18

Force10 Resilient Ring Protocol (FRRP)

Force10 Resilient Ring Protocol (FRRP) is supported on the S5000 switch.

FRRP is a proprietary protocol for that offers fast convergence in a Layer 2 network without having to run the Spanning Tree Protocol. The Resilient Ring Protocol is an efficient protocol that transmits a high-speed token across a ring to verify the link status. All the intelligence is contained in the master node with practically no intelligence required of the transit mode.

Important Points to Remember

- FRRP is media- and speed-independent.
- FRRP is a Dell Networking proprietary protocol that does not interoperate with any other vendor.
- Spanning Tree must be disabled on both primary and secondary interfaces before Resilient Ring protocol is enabled.
- A VLAN configured as the control VLAN for a ring cannot be configured as a control or member VLAN for any other ring.
- Member VLANs across multiple rings are not supported in Master nodes.
- If multiple rings share one or more member VLANs, they cannot share any links between them.
- Each ring can have only one Master node; all others are Transit nodes.

clear frrp

Clear the FRRP statistics counters.

S5000

Syntax

```
clear frrp [ring-id]
```

Parameters

ring-id	(Optional) Enter the ring identification number. Range: 1 to 255.

Defaults none

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Executing this command without the optional `ring-id` command clears the statistics counters on all the available rings. FTOS requires a command line confirmation before the command executes. This commands clears the following counters:

- hello Rx and Tx counters
- Topology change Rx and Tx counters
- The number of state change counters

Example

```
FTOS#clear frrp

Clear frrp statistics counter on all ring [confirm] yes

FTOS#clear frrp 4

Clear frrp statistics counter for ring 4 [confirm] yes

FTOS#
```

Related Commands

show frrp – displays the Resilient Ring Protocol configuration.

debug frrp

Clear the FRRP statistics counters.

S5000

Syntax

`debug frrp {event | packet | detail} [ring-id] [count number]`

To disable debugging, use the `no debug frrp {event | packet | detail} {ring-id} [countnumber]` command.

Parameters

event	Enter the keyword `event` to display debug information related to ring protocol transitions.
packet	Enter the keyword `packet` to display brief debug information related to control packets.
detail	Enter the keyword `detail` to display detailed debug information related to the entire ring protocol packets.
ring-id	(Optional) Enter the ring identification number. The range is 1 to 255.
count *number*	Enter the keyword `count` followed by the number of debug outputs. The range is 1 to 65534.

Defaults

Disabled

Command Modes

CONFIGURATION (conf-frrp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Because the resilient ring protocol can potentially transmit 20 packets per interface, you must restrict debug information.

member-vlan

Specify the member VLAN identification numbers.

S5000

Syntax `member-vlan {vlan-range}`

To return to the default, use the `no member-vlan [vlan-range]` command.

Parameters

vlan-range	Enter the member VLANs using VLAN IDs (separated by commas), a range of VLAN IDs (separated by a hyphen), a single VLAN ID, or a combination. For example: VLAN IDs (comma-separated): 3, 4, 6. Range (hyphen-separated): 5-10. Combination: 3, 4, 5-10, 8.

Defaults none

Command Modes CONFIGURATION (conf-frrp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

mode

Set the Master or Transit mode of the ring.

S5000

Syntax `mode {master | transit}`

To reset the mode, use the `no mode {master | transit}` command.

Parameters

master	Enter the keyword `master` to set the Ring node to Master mode.
transit	Enter the keyword`transit` to set the Ring node to Transit mode.

Defaults **Mode None**

Command Modes CONFIGURATION (conf-frrp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

protocol frrp

Enter the Resilient Ring Protocol and designate a ring identification.

S5000

Syntax `protocol frrp {ring-id}`

To exit the ring protocol, use the `no protocol frrp {ring-id}` command.

Parameters

ring-id	Enter the ring identification number. Range: 1 to 255.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This command places you into the resilient ring protocol. After executing this command, the command line prompt changes to `conf-frrp`.

show frrp

Display the Resilient Ring Protocol configuration.

S5000

Syntax `show frrp [ring-id [summary]] | [summary]`

Parameters

ring-id	Enter the ring identification number. The range is 1 to 255
summary	(OPTIONAL) Enter the keyword `summary` to view just a summarized version of the Ring configuration.

Defaults none

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Executing this command without the optional `ring-id` command clears the statistics counters on all the available rings. FTOS requires a command line confirmation before the command executes. This commands clears the following counters:

- hello Rx and Tx counters
- Topology change Rx and Tx counters
- The number of state change counters

Usage Information

Executing this command without the optional `ring-id` command clears the statistics counters on all the available rings. FTOS requires a command line confirmation before the command is executed. This commands clears the following counters:

- hello Rx and Tx counters
- Topology change Rx and Tx counters
- The number of state change counters

Example (Summary)

```
FTOS#show frrp summary

Ring-ID State Mode  Ctrl_Vlan Member_Vlans
----------------------------------------------
2       UP   Master   2        11-20, 25,27-30
31      UP   Transit  31       40-41
50      Down Transit  50       32
FTOS#
```

Example (1)

```
FTOS#show frrp 1
Ring protocol 1 is in Master mode
Ring Protocol Interface:
Primary : TenGigabitEthernet 0/16 State: Forwarding
Secondary: Port-channel 100 State: Blocking
Control Vlan: 1
Ring protocol Timers: Hello-Interval 50 msec Dead-Interval 150
msec
Ring Master's MAC Address is 00:01:e8:13:a3:19
Topology Change Statistics: Tx:110 Rx:45
Hello Statistics: Tx:13028 Rx:12348
Number of state Changes: 34
Member Vlans: 1000-1009
FTOS#
```

Example (2 Summary)

```
FTOS#show frrp 2 summary

FTOS#show frrp 2 summary
Ring-ID State Mode  Ctrl_Vlan Member_Vlans
-----------------------------------------------
2       Up    Master 2        11-20, 25, 27-30
FTOS#
```

Related Commands

protocol frrp — enters the resilient ring protocol and designate a ring identification.

19

GARP VLAN Registration (GVRP)

The basic GVRP commands are supported by FTOS on S5000 switch.

The generic attribute registration protocol (GARP) mechanism allows the configuration of a GARP participant to propagate through a network quickly. A GARP participant registers or de-registers its attributes with other participants by making or withdrawing declarations of attributes. At the same time, based on received declarations or withdrawals, GARP handles attributes of other participants.

GVRP enables a device to propagate local VLAN registration information to other participant devices and dynamically update the VLAN registration information from other devices. The registration information updates local databases regarding active VLAN members and through which port the VLANs can be reached.

GVRP ensures that all participants on a bridged LAN maintain the same VLAN registration information. The VLAN registration information propagated by GVRP include both manually configured local static entries and dynamic entries from other devices.

GVRP participants have the following components:

- The GVRP application
- GARP information propagation (GIP)
- GARP information declaration (GID)

Important Points to Remember

- GVRP is supported on Layer 2 ports only.
- All VLAN ports added by GVRP are tagged.
- GVRP is supported on untagged ports belonging to a default VLAN and tagged ports.
- GVRP cannot be enabled on untagged ports belonging to a non-default VLAN *unless* native VLAN is turned on.
- GVRP requires end stations with dynamic access NICs.
- Based on updates from GVRP-enabled devices, GVRP allows the system to dynamically create a port-based VLAN (unspecified) with a specific VLAN ID and a specific port.
- On a port-by-port basis, GVRP allows the system to learn about GVRP updates to an existing port-based VLAN with that VLAN ID and IEEE 802.1Q tagging.
- GVRP allows the system to send dynamic GVRP updates about your existing port-based VLAN.
- GVRP updates are not sent to any blocked spanning tree protocol (STP) ports. GVRP operates only on ports that are in the forwarding state.
- GVRP operates only on ports that are in the STP forwarding state. If GVRP is enabled, a port that changes to the STP forwarding state automatically begins to participate in GVRP. A port that changes to an STP state other than forwarding no longer participates in GVRP.
- VLANs created dynamically with GVRP exist only as long as a GVRP-enabled device is sending updates. If the devices no longer send updates, or GVRP is disabled, or the system is rebooted, all dynamic VLANs are removed.
- GVRP manages the active topology, not non-topological data such as VLAN protocols. If a local bridge needs to classify and analyze packets by VLAN protocols, you must manually configure protocol-based VLANs, and

simply rely on GVRP for VLAN updates. But if the local bridge needs to know only how to reach a given VLAN, then GVRP provides all necessary information.

- The VLAN topologies that GVRP learns are treated differently from VLANs that are statically configured. The GVRP dynamic updates are not saved in NVRAM, while static updates are saved in NVRAM. When GVRP is disabled, the system deletes all VLAN interfaces that were learned through GVRP and leaves unchanged all VLANs that were manually configured.

clear gvrp statistics

Clear GVRP statistics on an interface.

S5000

Syntax `clear gvrp statistics interface type slot/port`

Parameters

interface *type slot/port*	Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

Defaults none

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands show gvrp statistics – displays the GVRP statistics.

debug gvrp

Enable debugging on GVRP.

S5000

Syntax `debug gvrp {config | events | pdu}`

To disable debugging, use the `no debug gvrp {config | events | pdu}` command.

Parameters

config	Enter the keyword `config` to enable debugging on the GVRP configuration.
event	Enter the keyword `event` to enable debugging on the JOIN/LEAVE events.
pdu	Enter the keyword `pdu` followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

Defaults Disabled.

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

disable

Globally disable GVRP.

S5000

Syntax `disable`

To re-enable GVRP, use the `no disable` command.

Defaults Enabled.

Command Modes CONFIGURATION-GVRP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

gvrp enable – enables GVRP on physical interfaces and LAGs.

protocol gvrp – access GVRP protocol.

garp timers

Set the intervals (in milliseconds) for sending GARP messages.

S5000

Syntax

`garp timers {join | leave | leave-all}`

To return to the previous setting, use the `no garp timers {join | leave | leave-all}` command.

Parameters

join	Enter the keyword `join` followed by the number of milliseconds to configure the join time. The range is 100 to 147483647 milliseconds. The default is **200 milliseconds**. **NOTE:** Designate the milliseconds in multiples of 100.
leave	Enter the keyword `leave` followed by the number of milliseconds to configure the leave time. The range is 100 to 2147483647 milliseconds. The default is **600 milliseconds**. **NOTE:** Designate the milliseconds in multiples of 100.
leave-all	Enter the keywords `leave-all` followed by the number of milliseconds to configure the leave-all time. The range is 100 to 2147483647 milliseconds. The default is 1000 milliseconds. **NOTE:** Designate the milliseconds in multiples of 100.

Defaults

As above.

Command Modes

CONFIGURATION-GVRP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

- Join Timer—`Join` messages announce the willingness to register some attributes with other participants. For reliability, each GARP application entity sends a `Join` message twice and uses a join timer to set the sending interval.
- Leave Timer—`Leave` announces the willingness to de-register with other participants. Together with `Join`, `Leave` messages help GARP participants complete attribute reregistration and de-registration. The leave timer starts after receipt of a leave message sent for de-registering some attribute information. If a `Join` message is *not* received before the `Leave` time expires, the GARP application entity removes the attribute information as requested.
- Leave All Timer—The `Leave All` timer starts when a GARP application entity starts. When this timer expires, the entity sends a `Leave-all` message so that other entities can reregister their attribute information. Then the `Leave-all` time begins again.

Related Commands

show garp timers – displays the current GARP times.

gvrp enable

Enable GVRP on physical interfaces and LAGs.

S5000

Syntax

```
gvrp enable
```

To disable GVRP on the interface, use the `no gvrp enable` command.

Defaults

Disabled.

Command Modes

CONFIGURATION-INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

disable – globally disables GVRP.

gvrp registration

Configure the GVRP register type.

S5000

Syntax

```
gvrp registration {fixed | normal | forbidden}
```

To return to the default, use the `gvrp register normal` command.

Parameters

fixed	Enter the keyword `fixed` followed by the VLAN range in a comma separated VLAN ID set.
normal	Enter the keyword `normal` followed by the VLAN range in a comma separated VLAN ID set. This is the default.
forbidden	Enter the keyword `forbidden` followed by the VLAN range in a comma separated VLAN ID set.

Defaults

normal

Command Modes

CONFIGURATION-INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Fixed registration prevents an interface, configured using the command line, to belong to a VLAN (static configuration) from being unconfigured when it receives a `Leave` message. Therefore, Registration mode on that interface is fixed.

Normal registration is the default registration. The port's membership in the VLAN depends on GVRP. The interface becomes a member of a VLAN after learning about the VLAN through

GVRP. If the VLAN is removed from the port that sends GVRP advertisements to this device, the port stops being a member of the VLAN.

Use the `forbidden` command when you do not want the interface to advertise or learn about VLANs through GVRP.

Related Commands

show gvrp – displays the GVRP configuration including the registration.

protocol gvrp

Access GVRP protocol — (config-gvrp)#.

S5000

Syntax

```
protocol gvrp
```

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on S500.

Related Commands

disable – globally disables GVRP.

show config

Display the global GVRP configuration.

S5000

Syntax

```
show config
```

Command Modes

CONFIGURATION-GVRP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

gvrp enable – enables GVRP on physical interfaces and LAGs.

protocol gvrp – accesses the GVRP protocol.

show garp timers

Display the GARP timer settings for sending GARP messages.

S5000

Syntax `show garp timers`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show garp timers
GARP Timers       Value (milliseconds)
----------------------------------------
Join Timer         200
Leave Timer        600
LeaveAll Timer     10000
FTOS#
```

Related Commands garp timers – sets the intervals (in milliseconds) for sending GARP messages.

show gvrp

Display the GVRP configuration.

S5000

Syntax `show gvrp [brief | interface-type slot/port]`

Parameters

brief	(OPTIONAL) Enter the keyword `brief` to display a brief summary of the GVRP configuration.
interface-type slot/port	(OPTIONAL) Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If no ports are GVRP participants, the message output changes from `GVRP Participants running on <port_list>` to `GVRP Participants running on no ports.`

Example

```
R3#show gvrp brief
GVRP Feature is currently enabled.
Port                    GVRP Status      Edge-Port
----------------------------------------------
Te 3/0                  Disabled          No
Te 3/1                  Disabled          No
Te 3/2                  Enabled           No
Te 3/3                  Disabled          No
Te 3/4                  Disabled          No
Te 3/5                  Disabled          No
Te 3/6                  Disabled          No
Te 3/7                  Disabled          No
Te 3/8                  Disabled          No
R3#show gvrp brief
```

Related Commands show gvrp statistics – displays the GVRP statistics.

show gvrp statistics

Display the GVRP configuration statistics.

S5000

Syntax `show gvrp statistics {interface type slot/port | summary}`

Parameters

interface *type slot/port*	(OPTIONAL) Enter the keyword `interface` followed by the interface type and slot/ port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

summary	Enter the keyword `summary` to display just a summary of the GVRP statistics.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on S5000.

Usage Information

Invalid messages/attributes skipped can occur in the following cases:

- The incoming GVRP PDU has an incorrect length.
- "End of PDU" was reached before the complete attribute could be parsed.
- The Attribute Type of the attribute that was being parsed was not the GVRP VID Attribute Type (0x01).
- The attribute that was being parsed had an invalid attribute length.
- The attribute that was being parsed had an invalid GARP event.
- The attribute that was being parsed had an invalid VLAN ID. The valid range is 1 to 4095.

A failed registration can occur for the following reasons:

- `Join` requests were received on a port that was blocked from learning dynamic VLANs (GVRP Blocking state).
- An entry for a new GVRP VLAN could not be created in the GVRP database.

Example

```
FTOS#show gvrp statistics int te 1/0

Join Empty Received: 0
Join In Received: 0
Empty Received: 0
LeaveIn Received: 0
Leave Empty Received: 0
Leave All Received: 40
Join Empty Transmitted: 156
Join In Transmitted: 0
Empty Transmitted: 0
Leave In Transmitted: 0
Leave Empty Transmitted: 0
Leave All Transmitted: 41
Invalid Messages/Attributes skipped: 0
Failed Registrations: 0
FTOS#
```

Related Commands

show gvrp – displays the GVRP configuration.

20

High Availability (HA)

In FTOS, High Availability (HA) is a collection of features that synchronize switch configuration to minimize recovery time in the event of a stack-unit failure. High Availability features are supported only on stacked S5000 switches; they are not supported on a standalone S5000 switch.

In general, a protocol is defined as “hitless” in the context of stack-unit failure. A protocol is defined as hitless if a stack-unit failover has no impact on the protocol.

You must specifically enable some protocols for HA. Some protocols are only hitless if related protocols are also enabled as hitless (for example, the `redundancy protocol` command).

redundancy disable-auto-reboot

Prevent the system from auto-rebooting the failed stack-unit member(s).

S5000

Syntax

`redundancy disable-auto-reboot [stack-unit unit-number | members]`

To return to the default, use the `no redundancy disable-auto-reboot stack-unit` command.

Parameters

stack-unit *unit-number*	Enter the keyword `stack-unit` followed by number to disable auto-reboot of the failed stack-unit. The range is 0 to 11.
members	Enter the keyword `members` to disable auto-reboot of all members of the stack-unit.

Default

Disabled (that is, the failed module is automatically rebooted).

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Enabling this command keeps the failed stack-unit in the failed state. If there are two or more stack-unit members in the system, enabling this command prevents the failed stack-unit from becoming a standby unit. If there is only one stack-unit in the system, the failed unit does not recover and affects the system.

redundancy force-failover

Force the stand by stack-unit to become the primary stack-unit.

S5000

Syntax `redundancy force-failover {stack-unit}`

Parameters

stack-unit	Enter the keyword `stack-unit` to force a peer stack-unit to become the management stack-unit.

Default Not configured.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Use this command to provide a hitless or warm upgrade. A hitless upgrade means that a software upgrade requires a stack-unit to be reset but not rebooted. A warm upgrade is possible for major releases and lower, while a hitless upgrade can only support patch releases.

Example

```
FTOS#redundancy force-failover stack-unit
System configuration has been modified. Save? [yes/no]: yes
!
Jan 1 00:15:31: %STKUNIT2-M:CP %FILEMGR-5-FILESAVED: Copied
running-config to startup-config in flash by default
Synchronizing data to peer Stack-unit
!!!!

...
Proceed with Stack-unit hot failover [confirm yes/no]:yeJan 1
00:15:45: %STKUNIT2-M:CP %SYS-5-CONFIG_I: Configured from vty0
( 10.11.8.13 )by admin
s
f10StkATPResetReq: Requesting ATP reset from: 1 reason: 4
disableAutoReboot 0
syncing disks... done
unmounting file systems...
```

redundancy protocol

Enable hitless protocols.

S5000

Syntax `redundancy protocol {lacp | xstp}`

To disable a hitless protocol, use the `no redundancy protocol {lacp | xstp}` command.

Parameters	**lacp**	Enter the keyword `lacp` to make LACP hitless.
	xstp	Enter the keyword `xstp` to invoke hitless STP (all STP modes — MSTP, PVST+, RSTP, and STP).
Default	Disabled	
Command Modes	CONFIGURATION	
Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Related Commands

- show lacp – displays the lacp configuration.
- show redundancy – displays the current redundancy configuration.

redundancy reset-counter

Reset failover counter and timestamp information displayed in the `show redundancy` command.

S5000

Syntax	`redundancy reset-counter`	
Default	Not configured.	
Command Modes	EXEC Privilege	
Command History	**Version 9.0(1.3)**	Introduced on the S5000.

redundancy synchronize

Manually synchronize data between the primary stack-unit and the stand by stack-unit.

S5000

Syntax	`redundancy synchronize [full]`	
Parameters	**full**	Enter the keyword `full` to synchronize all data.
Default	Not configured.	
Command Modes	EXEC Privilege	

Command History

Version 9.0(1.3)	Introduced on the S5000.

show redundancy

Display the current redundancy configuration.

S5000

Syntax `show redundancy`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The following describes the `show redundancy` command shown in the Example below.

Field	**Description**
Stack-unit Status	Displays the following information: • Stack-unit ID. • Whether the stack-unit is a manaagement unit or standby. • The state of the stack-unit: Active, Standby, Booting, or Offline. • Whether the link to the peer stack-unit is up or down. • Whether a peer stack-unit is present or not and its state.
Stack-unit Redundancy Configuration	Displays the following information: • Which stack-unit is the preferred management unit on next boot • The data sync method configured (the `redundancy synchronize` command) • The failover type (you cannot change this type because it is software-dependent). **Hot Failover** means that the running configuration and routing table are applied on the peer stack-unit. **Fast Failover** means that the running configuration is not applied on the peer stack-unit until failover occurs, and the routing table on stack-units is cleared during failover. • The status of auto booting the stack-unit (the `redundancy disable-auto-reboot` command) • The parameter for auto failover limit control (the `redundancy auto-failover-limit` command)

Field	Description
	•
Stack-unit Failover Record	Displays the following information: • Stack-unit failover counter (to reset the counter, use the `redundancy reset-counter` command) • The time and date of the last stack-unit failover • The reason for the last stack-unit failover
Last Data Sync Record	Displays the data sync information and the timestamp for the data sync: • Stack-unit Config is configured stack-units and their interfaces. • Start-up Config is the contents of the startup-config file. • Runtime Event Log is the contents of the Event log. • Running Config is the current running-config. • ACL Mgr • LACP • STP • SPAN This field only appears when you enter the command from the management stack-unit.

Example

```
FTOS#show redundancy

--  Stack-unit Status  --
------------------------------------------------
 Mgmt ID:                         0
 Stack-unit ID:                   0
 Stack-unit Redundancy Role:      Primary
 Stack-unit State:                Active
 Stack-unit SW Version:           DIABLO-SYS-8-3-18-264
 Link to Peer:                    Down
 Peer Stack-unit:                 not present

--  Stack-unit Redundancy Configuration  --
------------------------------------------------
 Primary Stack-unit:              mgmt-id    0
 Auto Data Sync:                  Full
 Failover Type:                   Hot Failover
 Auto reboot Stack-unit:          Disabled
 Auto failover limit:             3 times in 60 minutes

--  Stack-unit Failover Record  --
------------------------------------------------
 Failover Count:                  0
 Last failover timestamp:         None
 Last failover Reason:            None
 Last failover type:              None

--  Last Data Block Sync Record:  --
------------------------------------------------
```

```
Stack Unit Config:  succeeded Jul 13 2012 21:28:53
Start-up Config:    succeeded Jul 13 2012 21:28:53
Runtime Event Log:  succeeded Jul 13 2012 21:28:53
Running Config:     succeeded Jul 13 2012 21:28:53
ACL Mgr:            succeeded Jul 13 2012 21:28:53
LACP:               succeeded Jul 13 2012 21:28:53
STP:                succeeded Jul 13 2012 21:28:53
SPAN:               succeeded Jul 13 2012 21:28:53
FTOS#
```

21

Internet Group Management Protocol (IGMP)

The IGMP commands are supported on the S5000 switch.

This chapter contains the following sections:

- IGMP Commands
- IGMP Snooping Commands

IGMP Commands

FTOS supports IGMPv1/v2/v3 and is compliant with RFC-3376.

Important Points to Remember

- FTOS supports protocol-independent multicast-sparse (PIM-SM) and protocol-independent source-specific multicast (PIM-SSM) include and exclude modes.
- IGMPv2 is the default version of IGMP on interfaces. You can configure IGMPv3 on interfaces. It is backward compatible with IGMPv2.
- The maximum number of interfaces supported is 31 on the S5000.
- There is no hard limit on the maximum number of groups supported.
- IGMPv3 router interoperability with IGMPv2 and IGMPv1 routers on the same subnet is not supported.
- An administrative command (`ip igmp version`) is added to manually set the IGMP version.
- All commands previously used for IGMPv2 are compatible with IGMPv3.

clear ip igmp groups

Clear entries from the group cache table.

S5000

Syntax `clear ip igmp groups [group-address | interface-type slot/port]`

Parameters

group-address	(OPTIONAL) Enter the IP multicast group address in dotted decimal format.
interface-type slot/port	Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below.

- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information IGMP commands accept *only* non-VLAN interfaces—specifying VLAN does not yield results.

debug ip igmp

Enable debugging of IGMP packets.

S5000

Syntax

```
debug ip igmp [group address | interface-type slot/port]
```

- To disable IGMP debugging, use the `no debug ip igmp [group address | interface]` command.
- To disable all debugging, use the `undebug all` command.

Parameters

group-address	(OPTIONAL) Enter the IP multicast group address in dotted decimal format.
interface-type slot/port	Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below.

- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults Disabled.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information IGMP commands accept *only* non-VLAN interfaces—specifying VLAN does not yield results. This command displays packets for IGMP and IGMP snooping.

ip igmp access-group

Use this feature to specify access control for packets.

S5000

Syntax `ip igmp access-group access-list`

To remove the feature, use the `no ip igmp access-group access-list` command.

Parameters

access-list	Enter the name of the extended ACL (16 characters maximum).

Defaults Not configured

Command Modes INTERFACE (conf-if-*interface-slot/port*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The access list accepted is an extended ACL. Use this feature to block IGMP reports from hosts, on a per-interface basis based on the group address and source address that you specify in the access list.

ip igmp group-join-limit

Use this feature to limit the number of IGMP groups that can be joined in a second.

S5000

Syntax `ip igmp group-join-limit number`

Parameters

number	Enter the number of IGMP groups permitted to join in a second. The range is 1 to 10000.

Defaults none

Command Modes CONFIGURATION (conf-if-*interface-slot/port*)

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

ip igmp immediate-leave

Enable IGMP immediate leave.

S5000

Syntax

`ip igmp immediate-leave [group-list prefix-list-name]`

To disable `ip igmp immediate leave`, use the `no ip igmp immediate-leave` command.

Parameters

group-list *prefix-list-name*	Enter the keywords `group-list` followed by a string up to 16 characters long of the prefix-list-name.

Defaults Not configured.

Command Modes INTERFACE

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Usage Information

Querier normally sends a certain number of group-specific queries when a `leave` message is received for a group prior to deleting a group from the membership database. There may be situations when you require immediate deletion of a group from the membership database. This command provides a way to achieve the immediate deletion. In addition, this command provides a way to enable `immediate-leave processing` for specified groups.

ip igmp last-member-query-interval

Change the last member query interval, which is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages. This interval is also the interval between Group-Specific Query messages.

S5000

Syntax

`ip igmp last-member-query-interval milliseconds`

To return to the default value, use the `no ip igmp last-member-query-interval` command.

Parameters

milliseconds	Enter the number of milliseconds as the interval. The range is 100 to 65535. The default is **1000 milliseconds**.

Defaults	**1000 milliseconds**
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ip igmp querier-timeout

Change the interval that must pass before a multicast router decides that there is no longer another multicast router that should be the querier.

S5000

Syntax

`ip igmp querier-timeout` *`seconds`*

To return to the default value, use the `no ip igmp querier-timeout` command.

Parameters

seconds	Enter the number of seconds the router must wait to become the new querier. The range is 60 to 300. The default is **125 seconds**.

Defaults	**125 seconds**
Command Modes	INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip igmp query-interval

Change the transmission frequency of IGMP general queries sent by the Querier.

S5000

Syntax

`ip igmp query-interval` *`seconds`*

To return to the default values, use the `no ip igmp query-interval` command.

Parameters

seconds	Enter the number of seconds between queries sent out. The range is 1 to 18000. The default is **60 seconds**.

Defaults	**60 seconds**
Command Modes	INTERFACE

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

ip igmp query-max-resp-time

Set the maximum query response time advertised in general queries.

S5000

Syntax `ip igmp query-max-resp-time` *`seconds`*

To return to the default values, use the `no ip igmp query-max-resp-time` command.

Parameters

seconds	Enter the number of seconds for the maximum response time. The range is 1 to 25. The default is **10 seconds**.

Defaults **10 seconds**

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip igmp ssm-map

Use a statically configured list to translate (*,G) memberships to (S,G) memberships.

S5000

Syntax `ip igmp ssm-map` *`std-access-list source-address`*

Undo this configuration, that is, remove SSM map (S,G) states and replace them with (*,G) state, use the `ip igmp ssm-map` *`std-access-list source-address`* command.

Parameters

std-access-list	Specify the standard IP access list that contains the mapping rules for multicast groups.
source-address	Specify the multicast source address to which the groups are mapped.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	Mapping applies to both v1 and v2 IGMP joins; any updates to the ACL are reflected in the IGMP groups. You may not use extended access lists with this command. When you configure a static SSM map and the router cannot find any matching access lists, the router continues to accept (*,G) groups.
Related Commands	ip access-list standard – creates a standard access list to filter based on IP address.

ip igmp static-group

Configure an IGMP static group.

S5000

Syntax

`ip igmp static-group {group address [exclude [source address]] | [include {source address}]}`

To delete a static address, use the `no ip igmp static-group {group address [exclude [source address]] | [include {source address}]}` command.

Parameters

group address	Enter the group address in dotted decimal format (A.B.C.D).
exclude *source address*	(OPTIONAL) Enter the keyword `exclude` followed by the source address, in dotted decimal format (A.B.C.D), for which a static entry needs to be added.
include *source address*	(OPTIONAL) Enter the keyword `include` followed by the source address, in dotted decimal format (A.B.C.D), for which a static entry needs to be added.

Defaults	none
Command Modes	INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

A group in `include` mode must have at least one source address defined. In `exclude` mode, if you do not specify a source address, FTOS implicitly assumes all sources are included. If you do not specify either `include` or `exclude`, FTOS implicitly assumes a IGMPv2 static join.

Command Limitations

- Only one mode (`include` or `exclude`) is permitted per multicast group per interface. To configure another mode, all sources belonging to the original mode must be unconfigured.
- If a static configuration is present and a packet for the same group arrives on an interface, the dynamic entry completely overwrites all the static configuration for the group.

Related Commands	show ip igmp groups – displays IGMP group information.

ip igmp version

Manually set the version of the router to IGMPv2 or IGMPv3.

S5000

Syntax

```
ip igmp version {2 | 3}
```

Parameters

2	Enter the number 2 to set the IGMP version number to IGMPv2.
3	Enter the number 3 to set the IGMP version number to IGMPv3.

Defaults **2** (that is, IGMPv2)

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip igmp groups

View the IGMP groups.

S5000

Syntax

```
show ip igmp groups [group-address [detail] | detail |
interface-type slot/port [group-address [detail]]]
```

Parameters

group-address	(OPTIONAL) Enter the group address in dotted decimal format to view information on that group only.
interface-type slot/port	(OPTIONAL) Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.

- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

detail	(OPTIONAL) Enter the keyword `detail` to display the IGMPv3 source information.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command displays the IGMP database, including configured entries for either all groups on all interfaces, all groups on specific interfaces, or specific groups on specific interfaces.

The following describes the `show ip igmp groups` command shown in the Example below.

Field	**Description**
Group Address	Lists the multicast address for the IGMP group.
Interface	Lists the interface type, slot and port number.
Mode	Displays the IGMP version used.
Uptime	Displays the amount of time the group has been operational.
Expires	Displays the amount of time until the entry expires.
Last Reporter	Displays the IP address of the last host to be a member of the IGMP group.
Member Ports	Indicates the port channel. If the port channel is VLT, an asterisk (*) after the port channel number indicates the port channel is locally down and that a remote VLT port is up.

Example

```
FTOS#show ip igmp groups
Total Number of Groups: 5
IGMP Connected Group Membership
Group Address Interface Mode Uptime Expires Last Reporter
225.0.0.0    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2
225.0.0.1    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2
225.0.0.2    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2
225.0.0.3    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2
225.0.0.4    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2
```

Example (VLT)

NOTE: The asterisk (*) after the port channel number (Po 2) highlighted in the Example below indicates the port channel is VLT, that the local VLT port channel is down and the remote VLT port is up.

```
FTOS#show ip igmp groups
Total Number of Groups: 5
IGMP Connected Group Membership
Group Address Interface Mode Uptime Expires Last Reporter
225.0.0.0    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2*
225.0.0.1    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2*
225.0.0.2    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2*
225.0.0.3    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2*
225.0.0.4    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2*
```

show ip igmp interface

View information on the interfaces participating in IGMP.

S5000

Syntax `show ip igmp interface [type slot/port]`

Parameters

interface *type slot/port*	(OPTIONAL) Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Usage Information

IGMP commands accept *only* non-VLAN interfaces—specifying VLAN does not yield results.

Example

```
FTOS#show ip igmp interface
TenGigabitEthernet 0/0 is down, line protocol is down
  Internet protocol processing disabled
TenGigabitEthernet 0/5 is down, line protocol is down
  Internet protocol processing disabled
TenGigabitEthernet 0/6 is down, line protocol is down
  Internet protocol processing disabled
TenGigabitEthernet 0/7 is up, line protocol is down
  Internet protocol processing disabled
TenGigabitEthernet 7/9 is up, line protocol is up
  Internet address is 10.87.5.250/24
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  IGMP last member query response interval is 1000 ms
  IGMP activity: 0 joins, 0 leaves
  IGMP querying router is 10.87.5.250 (this system)
  IGMP version is 2
```

show ip igmp ssm-map

Display is a list of groups that are currently in the IGMP group table and contain SSM mapped sources.

S5000

Syntax

```
show ip igmp ssm-map [group]
```

Parameters		
	group	(OPTIONAL) Enter the multicast group address in the form A.B.C.D to display the list of sources to which this group is mapped.

Command Modes

- EXEC
- EXEC Privilege

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Related Commands

ip igmp ssm-map – Uses a statically configured list to translate (*,G) memberships to (S,G) memberships.

IGMP Snooping Commands

FTOS supports IGMP Snooping version 2 and 3 on the S5000 switch.

Important Points to Remember for IGMP Snooping

- FTOS supports version 1, version 2, and version 3 hosts.
- FTOS IGMP snooping implementation is based on IP multicast address (not based on Layer 2 multicast mac address) and the IGMP snooping entries are in Layer 3 flow table not in Layer 2 forwarding information base (FIB).
- FTOS IGMP snooping implementation is based on draft-ietf-magma-snoop-10.
- IGMP snooping is not enabled by default on the switch.
- A maximum of 1800 groups and 600 VLAN are supported.
- IGMP snooping is not supported on a default VLAN interface.
- IGMP snooping is not supported over VLAN-Stack-enabled VLAN interfaces (you must disable IGMP snooping on a VLAN interface before configuring VLAN-Stack-related commands).
- IGMP snooping does not react to Layer 2 topology changes triggered by spanning tree protocol (STP).
- IGMP snooping reacts to Layer 2 topology changes triggered by multiple spanning tree protocol (MSTP) by sending a general query on the interface that comes in the FWD state.

Important Points to Remember for IGMP Querier

- The IGMP snooping Querier supports version 2.
- You must configure an IP address to the VLAN interface for IGMP snooping Querier to begin. The IGMP snooping Querier disables itself when a VLAN IP address is cleared, and then it restarts itself when an IP address is reassigned to the VLAN interface.
- When enabled, IGMP snooping Querier will not start if there is a statically configured multicast router interface in the VLAN.
- When enabled, IGMP snooping Querier starts after one query interval in case no IGMP general query (with IP SA lower than its VLAN IP address) is received on any of its VLAN members.
- When enabled, IGMP snooping Querier periodically sends general queries with an IP source address of the VLAN interface. If it receives a general query on any of its VLAN member, it checks the IP source address of the incoming frame.

  If the IP SA in the incoming IGMP general query frame is lower than the IP address of the VLAN interface, the switch disables its IGMP snooping Querier functionality.

  If the IP SA of the incoming IGMP general query is higher than the VLAN IP address, the switch continues to work as an IGMP snooping Querier.

ip igmp snooping enable

Enable IGMP snooping on all or a single VLAN. This is the master on/off switch to enable IGMP snooping.

S5000

Syntax	`ip igmp snooping enable` To disable IGMP snooping, use the `no ip igmp snooping enable` command.

Defaults Disabled.

Command Modes

- CONFIGURATION
- INTERFACE VLAN

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information You must enter this command to enable IGMP snooping. When you enable this from CONFIGURATION mode, IGMP snooping enables on all VLAN interfaces (except the default VLAN).

NOTE: You must execute the `no shutdown` command on the VLAN interface for IGMP Snooping to function.

Related Commands shutdown – (no shutdown) activates an interface.

ip igmp snooping fast-leave

Enable IGMP snooping fast-leave for this VLAN.

S5000

Syntax `ip igmp snooping fast-leave`

To disable IGMP snooping fast leave, use the `no igmp snooping fast-leave` command.

Defaults Not configured.

Command Modes INTERFACE VLAN — (conf-if-vl-*n*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Queriers normally send a certain number of queries when a leave message is received prior to deleting a group from the membership database. There may be situations when you require a fast deletion of a group. When you enable IGMP fast leave processing, the switch removes an interface from the multicast group as soon as it detects an IGMP version 2 leave message on the interface.

ip igmp snooping flood

This command controls the flooding behavior of unregistered multicast data packets.

S5000

Syntax	`ip igmp snooping flood`
Defaults	Enabled.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	On the S5000, unregistered multicast data traffic drops when you disable flooding; it does not forward the packets to multicast router ports. On the S5000, you must also disable Layer 3 multicast (`no ip multicast-routing`) in order to disable Layer 2 multicast flooding.

ip igmp snooping last-member-query-interval

The last member query interval is the maximum response time inserted into Group-Specific queries sent in response to Group-Leave messages.

S5000

Syntax	`ip igmp snooping last-member-query-interval` *`milliseconds`* To return to the default value, use the `no ip igmp snooping last-member-query-interval` command.
Parameters	***milliseconds*** Enter the interval in milliseconds. The range is 100 to 65535. The default is **1000 milliseconds**.
Defaults	**1000 milliseconds**
Command Modes	INTERFACE VLAN
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	This last-member-query-interval is also the interval between successive Group-Specific Query messages. Use this command to change the last-member-query interval.

ip igmp snooping mrouter

Statically configure a VLAN member port as a multicast router interface.

S5000

Syntax

`ip igmp snooping mrouter interface type slot/port`

To delete a specific multicast router interface, use the `no igmp snooping mrouter interface type slot/port` command.

Parameters

interface *type slot/port*	Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

Defaults

Not configured.

Command Modes

INTERFACE VLAN — (conf-if-vl-*n*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

FTOS provides the capability of statically configuring the interface to which a multicast router is attached. To configure a static connection to the multicast router, enter the `ip igmp snooping mrouter interface` command in the VLAN context. The interface to the router must be a part of the VLAN where you are entering the command.

ip igmp snooping querier

Enable IGMP querier processing for the VLAN interface.

S5000

Syntax

`ip igmp snooping querier`

To disable IGMP querier processing for the VLAN interface, use the `no ip igmp snooping querier` command.

Defaults

Not configured.

Command Modes

INTERFACE VLAN — (conf-if-vl-*n*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This command enables the IGMP switch to send General Queries periodically. This is useful when there is no multicast router present in the VLAN because the multicast traffic does not need to be routed. You must assign an IP address to the VLAN interface for the switch to act as a querier for this VLAN.

show ip igmp snooping mrouter

Display multicast router interfaces.

S5000

Syntax `show ip igmp snooping mrouter [vlan number]`

Parameters

vlan ***number***	Enter the keyword `vlan` followed by the vlan number. The range is 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If the port channel is a VLT port channel, an asterisk (*) after the port channel number (Po 100*) indicates the port channel is locally down and that a remote VLT port is up.

Example

```
FTOS#show ip igmp snooping mrouter
Interface Router Ports
Vlan 2 Gi 13/3, Po 1
FTOS#
```

Related Commands

- ip igmp snooping mrouter – Use this command to configure a static connection to the multicast router.
- show ip igmp groups – use this IGMP command to view groups.

22

Interfaces

The commands in this chapter are supported in FTOS on the S5000 switch.

This chapter contains the following sections:

- Basic Interface Commands
- Port Channel Commands
- Time Domain Reflectometer (TDR)
- UDP Broadcast

Basic Interface Commands

The following commands are for Physical, Loopback, and Null interfaces.

clear counters

Clear the counters used in the show interfaces commands for all virtual router redundancy protocol (VRRP) groups, virtual local area networks (VLANs), and physical interfaces, or selected ones.

S5000

Syntax

```
clear counters [interface-type slot/port] [vrrp [{[ipv6]
vrid }] | learning-limit]
```

Parameters

interface-type slot/port: (OPTIONAL) Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below.

- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
- For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0.

- For the management interface on the stack-unit, enter the keyword `ManagementEthernet` followed by slot number (0-1) and port number zero (0).
- For a Fibre Channel interface, enter the keyword `fibrechannel` followed by slot/port numbers. The port range is 0 to 47.

vrrp [[ipv6] *vrid*]	(OPTIONAL) Enter the keyword `vrrp` to clear the counters of all VRRP groups. To clear the counters of VRRP groups on all IPv6 interfaces, enter `ipv6`. To clear the counters of a specified group, enter a VRID number from 1 to 255.
learning-limit	(OPTIONAL) Enter the keywords `learning-limit` to clear unknown source address (SA) drop counters when MAC learning limit is configured on the interface.

Defaults Without an interface specified, the command clears all interface counters.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#clear counters
Clear counters on all interfaces [confirm]
```

Related Commands show interfaces – displays information on the interfaces.

clear dampening

Clear the dampening counters on all the interfaces or just the specified interface.

S5000

Syntax `clear dampening [interface-type slot/port]`

Parameters

interface-type slot/port	(OPTIONAL) Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below.

- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

Defaults

Without an interface specified, the command clears all interface dampening counters.

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

After you enter the `clear counters` command and verify the results with the `show interfaces` command, the line rate is not reset to 0.00%.

Example

```
FTOS#clear dampening tengigabitethernet 1/2
Clear dampening counters on Te 1/2 [confirm] y
FTOS#
```

Related Commands

show interfaces dampening – displays interface dampening information.

dampening – configures dampening on an interface.

cx4-cable-length

Configure the length of the cable to be connected to the selected CX4 port.

S5000

Syntax

```
[no] cx4-cable-length {long | medium | short}
```

Parameters

long | medium | short	Enter the keyword that matches the cable length to be used at the selected port: • `short` = For 1-meter and 3-meter cable lengths. • `medium` = For 5-meter cable length. • `long` = For 10-meter and 15-meter cable lengths.

Defaults

medium

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command only works on ports that the system recognizes as CX4 ports. The `show interfaces` command shown in the Example below describes an attempt to configure an XFP port in an S25P with the command after inserting a CX4 converter into the port.

NOTE: When using a long CX4 cable, to avoid errors, configure the cable using the cx4-cable-length `short` command only.

NOTE: The 15M CX4 active cable is not supported on the S5000.

NOTE: For information about using XFP ports with CX4 cables, refer to your S5000 hardware guide.

Example (Unsuccessful)

```
FTOS#show interfaces tengigabitethernet 0/26 | grep "XFP type"

Pluggable media present, XFP type is 10GBASE-CX4

FTOS(conf-if-te-0/26)#cx4-cable-length short
% Error: Unsupported command.
FTOS(conf-if-te-0/26)#cx4-cable-length medium
% Error: Unsupported command.
FTOS(conf-if-te-0/26)#cx4-cable-length long
% Error: Unsupported command.
FTOS(conf-if-te-0/26)#
```

Example (Successful)

```
FTOS#config
FTOS(config)#interface tengigabitethernet 0/52
FTOS(conf-if-0/52)#cx4-cable-length long
FTOS(conf-if-0/52)#show config
!
interface TenGigabitEthernet 0/51
  no ip address
  cx4-cable-length long
  shutdown
FTOS(conf-if-0/52)#exit
FTOS(config)#
```

Related Commands

show config – displays the configuration of the selected interface.

dampening

Configure dampening on an interface.

S5000

Syntax

`dampening [[[[half-life] [reuse-threshold]] [suppress-threshold]] [max-suppress-time]]`

Parameters

half-life	Enter the number of seconds after which the penalty is decreased. The penalty is decreased by half after the half-life period expires. The range is 1 to 30 seconds. The default is **5 seconds**.
reuse-threshold	Enter a number as the reuse threshold, the penalty value below which the interface state is changed to “up”. The range is 1 to 20000. The default is **750**.
suppress-threshold	Enter a number as the suppress threshold, the penalty value above which the interface state is changed to “error disabled”. The range is 1 to 20000. The default is **2500**.
max-suppress-time	Enter the maximum number for which a route can be suppressed. The default is four times the half-life value. The range is 1 to 86400. The default is **20 seconds**.

Defaults Disabled.

Command Modes INTERFACE (conf-if-)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

With each flap, FTOS penalizes the interface by assigning a penalty (1024) that decays exponentially depending on the configured half-life. After the accumulated penalty exceeds the suppress threshold value, the interface moves to the Error-Disabled state. This interface state is deemed as “down” by all static/dynamic Layer 2 and Layer 3 protocols. The penalty is exponentially decayed based on the half-life timer. After the penalty decays below the reuse threshold, the interface enables. The configured parameters are as follows:

- `suppress-threshold` should be greater than `reuse-threshold`
- `max-suppress-time` should be at least 4 times `half-life`

NOTE: You cannot apply dampening on an interface that is monitoring traffic for other interfaces.

Example

```
FTOS(conf-if-te-3/2)#dampening 20 800 4500 120
FTOS(conf-if-te-3/2)#
```

Related Commands

clear dampening – clears the dampening counters on all the interfaces or just the specified interface.

show interfaces dampening – displays interface dampening information.

description

Assign a descriptive text string to the interface.

S5000

Syntax `description` *`desc_text`*

To delete a description, use the `no description` command.

Parameters

desc_text	Enter a text string up to 240 characters long.

Defaults none

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Important Points:

- Spaces between characters are not preserved after entering this command unless you enclose the entire description in quotation marks (“*`desc_text`*”).

- Entering a text string after the `description` command overwrites any previous text string that you previously configured as the description.
- The `shutdown` and `description` commands are the only commands that you can configure on an interface that is a member of a port-channel.
- Use the `show interfaces description` command to display descriptions configured for each interface.

Related Commands

show interfaces description – displays the description field of the interfaces.

duplex (Management interface)

Configure duplex mode on a management interface whose speed is set to 10/100 Mb/s.

S5000

Syntax

```
duplex {half | full}
```

To return to the default setting, use the `no duplex` command.

Parameters

half	Enter the keyword `half` to set the physical interface to transmit only in one direction.
full	Enter the keyword `full` to set the physical interface to transmit in both directions.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command applies only to management interfaces with speed set to 10/100 Mb/s using the `speed` command.

NOTE: When you set the speed to 10 or 100 Mbps, you can also execute the `duplex` command.

Related Commands

interface ManagementEthernet — configures the Management port on the system (either the primary or standby stack-unit)

negotiation auto – enables or disables auto-negotiation on an interface.

ecmp-group

Provides a mechanism to monitor traffic distribution on a link aggregation group (LAG) bundle. A system log or simple network management protocol (SNMP) trap is generated when the standard deviation of traffic distribution on a member link exceeds a defined threshold.

S5000

Syntax

`ecmp-group {ecmp-path} [interface interface] [monitoring enable]`

To negate a command, use the `no` command.

Parameters

ecmp-path	Enter the path number for the LAG. The range is 2 to 64.
interface	Enter the following keywords and slot/port to add the interface to the LAG: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
monitoring	Enter the keyword `monitoring` to monitor the LAG. To enable monitoring, follow by entering the keyword `enable`.

Defaults Off

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

flowcontrol

Set how the system responds to and generates 802.3x pause frames on Ethernet interfaces.

S5000

Syntax

`flowcontrol rx {off | on} tx {off | on}`

Parameters

rx on	Enter the keywords `rx on` to process the received flow control frames on this port. This is the default value for the receive side.
rx off	Enter the keywords `rx off` to ignore the received flow control frames on this port.

tx on	Enter the keywords `tx on` to send control frames from this port to the connected device when a higher rate of traffic is received. This is the default value on the send side.
tx off	Enter the keywords `tx off` so that flow control frames are not sent from this port to the connected device when a higher rate of traffic is received.

Defaults rx off tx off

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The globally assigned 48-bit Multicast address 01-80-C2-00-00-01 is used to send and receive pause frames. To allow full-duplex flow control, stations implementing the pause operation instruct the MAC to enable the reception of frames with a destination address equal to this multicast address.

An Ethernet interface starts to send pause frames to a sending device when the transmission rate of ingress traffic exceeds the egress port speed. The interface stops sending pause frames when the ingress rate falls to less than or equal to egress port speed.

Changes in the flow-control values may not be reflected automatically in `show interface` output. To display the change, apply the new flow-control setting, perform a `shutdown` followed by a `no shutdown` on the interface, and then check re-display the `show interface` output for the port.

Important Points to Remember

- On the S5000, Ethernet Pause Frame flow control is not supported if PFC is enabled on one or more interfaces.
- On the S5000, threshold settings on the transmission pause (tx on) are not supported for Ethernet Pause Frame flow control.
- Do not enable `tx pause` when buffer carving is enabled. For information and assistance, contact Dell Networking TAC.

NOTE: If you `disable rx flow control`, Dell Networking recommends rebooting the system.

Example

```
FTOS(conf-if-gi-0/1)#show config
!
interface GigabitEthernet 0/1
no ip address
switchport
no negotiation auto
flowcontrol rx off tx on
no shutdown
...
```

Example (Values)

This Example shows how FTOS negotiates the flow control values between two switches connected back-to-back using 1G copper ports.

```
Configured

LocRxConf LocTxConf RemoteRxConf RemoteTxConf
off       off        off           off
```

```
                     off           on
                     on            off
                     on            on

off       on         off           off
                     off           on
                     on            off
                     on            on

on        off        off           off
                     off           on
                     on            off
                     on            on

on        on         off           off
                     off           on
                     on            off
                     on            on

LocNegRx LocNegTx RemNegRx RemNegTx
off      off     off      off
off      off     off      off
off      off     off      off
off      off     off      off

off      off     off      off
off      off     off      off
off      on      on       off
off      off     off      off

off      off     off      off
on       off     off      on
on       on      on       on
on       on      on       on

off      off      off     off
off      off      off     off
on       on       on      on
on       on       on      on
```

Related Commands

show running-config – displays the flow configuration parameters (non-default values only).

show interfaces – displays the negotiated flow control parameters.

interface

Configure a physical interface on the switch.

S5000

Syntax

```
interface type slot/port
```

Parameters

interface *type slot/port*	Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below.

- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a range of interfaces, enter the keyword `range` followed by slot/port number.
- For a Fibre Channel interface, enter the keyword `FibreChannel` followed by slot/port numbers. The port range is 0 to 47.
- For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
- For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0.
- For a Null interface, enter the keywords `null 0`.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You cannot delete a physical interface.

By default, physical interfaces are disabled (`shutdown`) and are in Layer 3 mode. To place an interface in Layer 2 mode, ensure that the interface’s configuration does not contain an IP address and enter the `switchport` command.

Example

```
FTOS(conf)#interface te 0/0
FTOS(conf-if-te-0/0)#
```

Related Commands

interface fibrechannel — configures a Fibre Channel interface.

interface loopback – configures a Loopback interface.

interface null – configures a Null interface.

interface port-channel – configures a port channel.

interface vlan – configures a VLAN.

show interfaces – displays the interface configuration.

interface loopback

Configure a Loopback interface.

S5000

Syntax

`interface loopback number`

To remove a loopback interface, use the `no interface loopback number` command.

Parameters

number	Enter a number as the interface number. The range is 0 to 16383.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf)#interface loopback 1655
FTOS(conf-if-lo-1655)#
```

Related Commands

interface – configures a physical interface.

interface null – configures a Null interface.

interface port-channel – configures a port channel.

interface vlan – configures a VLAN.

interface ManagementEthernet

Configure the Management port on the system (either the primary or standby stack-unit).

S5000

Syntax

`interface ManagementEthernet slot/port`

Parameters

slot/port	Enter the keyword `ManagementEthernet` followed by slot/port information. Slot range is 0 to 1. Port number is 0.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You cannot delete a Management port.

The Management port is enabled by default (`no shutdown`). Use the `ip address` command to assign an IP address to the Management port.

If your system has more than one stack-unit, use the `show redundancy` command to display which stack-unit is the primary unit.

Example

```
FTOS(conf)#interface managementethernet 0/0
FTOS(conf-if-ma-0/0)#
```

Related Commands

management route – configures a static route that points to the Management interface or a forwarding router.

duplex (Management) – clears the forwarding information base (FIB) entries on a specified stack-unit.

speed (Management interface) – clears the FIB entries on a specified stack-unit.

interface null

Configure a Null interface on the switch.

S5000

Syntax

```
interface null number
```

Parameters

number	Enter zero (0) as the Null interface number.

Defaults

Not configured; number = **0**

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You cannot delete the Null interface. The only configuration command possible in a Null interface is `ip unreachables`.

Example

```
FTOS(conf)#interface null 0
FTOS(conf-if-nu-0)#
```

Related Commands

interface – configures a physical interface.

interface loopback – configures a Loopback interface.

interface port-channel – configures a port channel.

interface vlan – configures a VLAN.

ip unreachables – enables generation of internet control message protocol (ICMP) unreachable messages.

interface range

This command permits configuration of a range of interfaces to which subsequent commands are applied (bulk configuration). Using the `interface range` command, you can enter identical commands for a range of interface.

S5000

Syntax

`interface range` *interface-type slot/port—range , - interface-type slot/port—range , ...*

Parameters

interface range ***port-type slot/ port , port-type slot/port , ...***

Enter the keywords `interface range` followed by the interface type, slot number (if necessary), and a port range. Valid slot numbers are 0-11. The valid port numbers for each interface type are:

- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by a port number. The port numbers are 48, 52, 56, and 60.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
- For a Fibre Channel interface, enter the keyword `FibreChannel` followed by slot/port numbers. The port range is 0 to 47.

A port range must contain a space before and after the dash; for example: `interface range tengigabitethernet 0/1 - 5` is valid; `interface range tengigabitethernet 0/1-5` is not valid.

You can enter up to six comma-separated ranges. Separate each interface type and port range with a space, comma, and space; for example: `interface range tengigabitethernet 0/1 - 5 , interface range tengigabitethernet 0/10 - 11`.

Comma-separated port ranges can include VLANs, port-channels, and physical interfaces; for example: `interface range tengigabitethernet 0/1 - 5 , vlan 2 – 10 , port—channel 1 – 5`.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When creating an interface range, interfaces appear in the order they are entered; they are not sorted. The command verifies that interfaces are present (physical) or configured (logical).

Important Things to Remember:

- Bulk configuration is created if at least one interface is valid.
- Non-existing interfaces are excluded from the bulk configuration with a warning message.
- The `interface range` prompt includes interface types with slot/port information for valid interfaces. The prompt allows for a maximum of 32 characters. If the bulk configuration exceeds 32 characters, it is represented by an ellipsis (...).
- When the `interface range` prompt has multiple port ranges, the smaller port range is excluded from the prompt.
- If overlapping port ranges are specified, the port range is extended to the smallest start port and the biggest end port.

Example (Bulk)

```
FTOS(conf)#interface range fc 0/0 - 5 , te 1/12 - 23 , te 3/36
- 47
% Warning: Non-existing ports (not configured) are ignored by
interface-range
```

Example (Multiple Ports)

```
FTOS(conf)#interface range te 1/12 - 23 , te 2/24 - 30
FTOS(conf-if-range-te-1/12-23,te-2/24-30)#
```

Example (Overlapping Ports)

```
FTOS(conf)#interface range te 2/12 - 16 , te 2/12 - 23
FTOS(conf-if-range-te-2/12-23)#
```

Usage Information

Only VLAN and port-channel interfaces created using the `interface vlan` and `interface port-channel` commands can be used in the `interface range` command.

Use the `show running-config` command to display the VLAN and port-channel interfaces. VLAN or port-channel interfaces that are not displayed in the `show running-config` command can not be used with the bulk configuration feature of the `interface range` command. You cannot create virtual interfaces (VLAN, Port-channel) using the `interface range` command.

NOTE: If a range has VLAN, physical, and port-channel, interfaces, only commands related to physical interfaces can be bulk configured. To configure commands specific to VLANs or port-channels, only those respective interfaces should be configured in a particular range.

Example (Single Range)

This example shows a single range bulk configuration.

```
FTOS(config)# interface range tengigabitethernet 3/36 - 47
FTOS(config-if-range-te-3/36-47)# no shutdown
FTOS(config-if-range)#
```

Example (Multiple Range)

This example shows how to use commas to add different interface types to the range enabling all Ten Gigabit Ethernet interfaces in the range 0/0 to 0/11 and two Forty Gigabit Ethernet interfaces 48 and 52.

```
FTOS(config-if)# interface range gigabitethernet 0/0 - 11 ,
fortygigabitethernet 48 - 52
FTOS(config-if-range-te-0/0-11,fo-48-52)# no shutdown
FTOS(config-if-range)#
```

Example (Multiple Range)

This example shows how to use commas to add VLAN and port-channel interfaces to the range.

```
FTOS(config-if)# interface range gigabitethernet 2/24 - 35 ,
tengigabitethernet 3/36 - 41 ,
vlan 2 - 100 , port-channel 1 - 25
FTOS(config-if-range-gi-2/24-35,te-3/36-41,vl-2-100,po-1-25)#
no shutdown
FTOS(config-if-range)#
```

Related Commands

interface port-channel – configures a port channel group.

interface vlan – configures a VLAN interface.

show config (from INTERFACE RANGE mode) – shows the bulk configuration interfaces.

show range – shows the bulk configuration ranges.

interface range macro (define) – defines a macro for an interface-range.

interface range macro (define)

Defines a macro for an interface range and then saves the macro in the running configuration.

S5000

Syntax

```
define interface-range macro-name type slot/port - port, ...
```

Parameters

macro name	Enter up to 16 characters for the macro name.
interface range *type slot/port - port, ...*	Use the `define` command, and enter the keywords `interface range` followed by the macro name, interface type, and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are: - For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by a port number. The port numbers are 48, 52, 56, and 60. - For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. - For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094. - For a Fibre Channel interface, enter the keyword `FibreChannel` followed by slot/port numbers. The port range is 0 to 47. A port range must contain a space before and after the dash; for example: `interface range tengigabitethernet 0/1 - 5` is valid; `interface range tengigabitethernet 0/1-5` is not valid.

You can enter up to six comma-separated ranges. Separate each interface type and port range with a space, comma, and space; for example: `interface range tengigabitethernet 0/1 - 5 , interface range tengigabitethernet 0/10 - 11`.

Comma-separated port ranges can include VLANs, port-channels, and physical interfaces; for example: `interface range tengigabitethernet 0/1 - 5 , vlan 2 – 10 , port—channel 1 – 5`.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (Single Range)

This example shows how to define an interface range macro named test. Execute the `show running-config` command to display the macro definition.

```
FTOS(config)# define interface-range test tengigabitethernet
0/0 - 3, gigabitethernet 0/10 - 11, tengigabitethernet 1/12 -
20
FTOS# show running-config | grep define
define interface-range test tengigabitethernet 0/0 - 3,
gigabitethernet 0/10 - 11, tengigabitethernet 1/12 - 20
FTOS(config)#interface range macro test
FTOS(config-if-range-te-0/0-3,gi-0/10-11,te-1/12-20)#
```

Related Commands

interface range – configures a range of command (bulk configuration)

interface range macro name – runs an interface range macro.

interface range macro name

Run the interface-range macro to automatically configure the pre-defined range of interfaces.

S5000

Syntax `interface range macro` *`macro-name`*

Parameters

macro ***macro-name***	Enter the name of an existing macro.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (Single Range)

This example shows the macro named *test* that was defined earlier.

```
FTOS(config)#interface range macro test
FTOS(config-if-range-te-0/0-3,gi-5/0-47,gi-13/0-89)#
FTOS
```

Related Commands

interface range – configures a range of command (bulk configuration).

interface range macro (define) – defines a macro for an interface range (bulk configuration).

interface vlan

Configure a VLAN. You can configure up to 4094 VLANs.

S5000

Syntax

```
interface vlan vlan-id
```

Parameters

vlan-id	Enter a number as the VLAN Identifier. The range is 1 to 4094.

Defaults

Not configured, except for the Default VLAN, which is configured as VLAN 1.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

For more information about VLANs and the commands to configure them, refer to the Virtual LAN (VLAN) Commands section of the Layer 2 chapter.

FTP, TFTP, and SNMP operations are not supported on a VLAN. MAC ACLs are not supported in VLANs. IP ACLs are supported. For more information, refer to the Access Control Lists (ACL) chapter.

Example (Single Range)

```
FTOS(conf)#int vlan 3
FTOS(conf-if-vl-3)#
```

Related Commands

interface – configures a physical interface.

interface loopback – configures a loopback interface.

interface null – configures a null interface.

interface port-channel – configures a port channel group.

show vlan – displays the current VLAN configuration on the switch.

shutdown – disables/enables the VLAN.

tagged – adds a Layer 2 interface to a VLAN as a tagged interface.

untagged – adds a Layer 2 interface to a VLAN as an untagged interface.

keepalive

Send keepalive packets periodically to keep an interface alive when it is not transmitting data.

S5000

Syntax

`keepalive [`*`seconds`*`]`

To stop sending keepalive packets, use the `no keepalive` command.

Parameters

seconds	(OPTIONAL) Enter the number of seconds between keepalive packets. The range is 0 to 23767. The default is **10 seconds**.

Defaults

Enabled.

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you configure `keepalive`, the system sends a self-addressed packet out of the configured interface to verify that the far end of a WAN link is up. When you configure `no keepalive`, the system does not send keepalive packets and so the local end of a WAN link remains up even if the remote end is down.

monitor interface

Monitor counters on a single interface or all interfaces on a stack-unit. The screen is refreshed every five seconds and the CLI prompt disappears.

S5000

Syntax

`monitor interface [`*`type slot/port`*` | stack-unit `*`unit-number`*`]`

To disable monitoring and return to the CLI prompt, press the `q` key.

Parameters

interface*type slot/port*	(OPTIONAL) Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For the management port, enter the keyword `managementethernet` followed by the slot (0-1) and the port (0).

- For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

stack-unit *unit-number*	(OPTIONAL) Enter the `stack-unit` keyword followed by the unit number. The range is 0 to 11.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

In the Example, the delta column displays changes since the last screen refresh.

The following are the `monitor` command menu options.

systest-3	Displays the host name assigned to the system.
monitor time	Displays the amount of time since the `monitor interface` command was entered.
time	Displays the amount of time the chassis is up (since last reboot).
m	Change the view from a single interface to all interfaces on the stack-unit or visa-versa.
c	Refresh the view.
b	Change the counters displayed from Packets on the interface to Bytes.
r	Change the [delta] column from change in the number of packets/bytes in the last interval to rate per second.
l	Change the view to the next interface on the stack-unit.
a	Change the view to the previous interface on the stack-unit.
T	Increase the screen refresh rate.
t	Decrease the screen refresh rate.
q	Return to the CLI prompt.

Example (single interface)

```
FTOS# monitor interface te 0/1


systest-3 Monitor time: 00:00:06 Refresh Intvl.: 2s Time:
03:26:26

Interface: Te 0/1, Enabled, Link is Up, Linespeed is 1000 Mbit

Traffic statistics:    Current    Rate     Delta
```

```
       Input bytes:    9069828  43 Bps     86
      Output bytes:  606915800  43 Bps     86
     Input packets:      54001   0 pps      1
    Output packets:    9401589   0 pps      1
       64B packets:         67   0 pps      0
  Over 64B packets:      49166   0 pps      1
 Over 127B packets:        350   0 pps      0
 Over 255B packets:       1351   0 pps      0
 Over 511B packets:        286   0 pps      0
Over 1023B packets:       2781   0 pps      0
  Error statistics:
   Input underruns:          0   0 pps      0
      Input giants:          0   0 pps      0
   Input throttles:          0   0 pps      0
         Input CRC:          0   0 pps      0
 Input IP checksum:          0   0 pps      0
     Input overrun:          0   0 pps      0
  Output underruns:          0   0 pps      0
  Output throttles:          0   0 pps      0

  m - Change mode                c - Clear screen
  l - Page up                    a - Page down
  T - Increase refresh interval  t - Decrease refresh interval
  q - Quit
```

Example (all interfaces)

```
FTOS# monitor interface

systest-3 Monitor time: 00:01:31 Refresh Intvl.: 2s Time:
03:54:14

Interface  Link  In Packets  [delta]  Out Packets  [delta]

   Te 0/0  Down           0        0            0        0
   Te 0/1  Down           0        0            0        0
   Te 0/2  Up         61512       52        66160       42
   Te 0/3  Up         63086       20      9405888       24
   Te 0/4  Up   14697471418  2661481  13392989657  2661385
   Te 0/5  Up          3759        3    161959604   832816
   Te 0/6  Up          4070        3      8680346        5
   Te 0/7  Up         61934       34    138734357       72
   Te 0/8  Up         61427        1        59960        1
   Te 0/9  Up         62039       53    104239232        3
   Te 0/10 Up   17740044091      372   7373849244       79
   Te 0/11 Up   18182889225       44   7184747584      138
   Te 0/12 Up   18182682056        0         3682        1
   Te 0/13 Up   18182681434       43   6592378911      144
   Te 0/14 Up         61349       55     86281941       15
   Te 0/15 Up         59808       58        62060       27
   Te 0/16 Up         59889        1        61616        1
   Te 0/17 Up             0        0     14950126    81293
   Te 0/18 Up             0        0            0        0
   Te 0/19 Down           0        0            0        0
   Te 0/20 Up         62734       54        62766       18
   Te 0/21 Up         60198        9       200899        9
   Te 0/22 Up   17304741100  3157554  10102508511  1114221
   Te 0/23 Up   17304769659  3139507   7133354895   523329

m - Change mode               c - Clear screen
b - Display bytes             r - Display pkts/bytes per sec
l - Page up                   a - Page down
T - Increase refresh interval t - Decrease refresh interval
q - Quit
```

mtu

Set the link maximum transmission unit (MTU) (frame size) for an Ethernet interface.

S5000

Syntax

`mtu value`

To return to the default MTU value, use the `no mtu` command.

Parameters

value	Enter a maximum frame size in bytes. The range is 594 to 12000. The default is **1554**.

Defaults **1554**

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If the packet includes a Layer 2 header, the difference between the link MTU and IP MTU (`ip mtu` command) must be enough bytes to include the Layer 2 header:

When you enter the `no mtu` command, FTOS reduces the IP MTU value to 1536 bytes.

Link MTU and IP MTU considerations for port channels and VLANs are as follows.

port channels:

- All members must have the same link MTU value and the same IP MTU value.
- The port channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members. For example, if the members have a link MTU of 2100 and an IP MTU 2000, the port channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

VLANs:

- All members of a VLAN must have same IP MTU value.
- Members can have different Link MTU values. Tagged members must have a link MTU 4 bytes higher than untagged members to account for the packet tag.
- The VLAN link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the VLAN members. For example, the VLAN contains tagged members with Link MTU of 1522 and IP MTU of 1500 and untagged members with Link MTU of 1518 and IP MTU of 1500. The VLAN's Link MTU cannot be higher than 1518 bytes and its IP MTU cannot be higher than 1500 bytes.

The following shows the difference between Link MTU and IP MTU.

Layer 2 Overhead	Link MTU and IP MTU Delta
Ethernet (untagged)	18 bytes
VLAN Tag	22 bytes
Untagged Packet with VLAN-Stack Header	22 bytes

Layer 2 Overhead	Link MTU and IP MTU Delta
Tagged Packet with VLAN-Stack Header	26 bytes

portmode hybrid

Set a physical port or port-channel to accept both tagged and untagged frames. A port configured this way is identified as a hybrid port in report displays.

S5000

Syntax

`portmode hybrid`

To return a port to accept either tagged or untagged frames (non-hybrid), use the `no portmode hybrid` command.

Defaults

non-hybrid

Command Modes

INTERFACE (conf-if-interface-slot/port)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `interface` command shown in the Example below. This example sets a port as hybrid, makes the port a tagged member of VLAN 20, and an untagged member of VLAN 10, which becomes the native VLAN of the port. The port will now accept:

- untagged frames and classify them as VLAN 10 frames
- VLAN 20 tagged frames

The following describes the `do show interfaces` command shown in the Example below. This example shows output with “Hybrid” as the newly added value for 802.1QTagged. The options for this field are:

- True—port is tagged
- False—port is untagged
- Hybrid—port accepts both tagged and untagged frames

The following describes the `interface vlan` command shown in the Example below. This example shows unconfiguration of the hybrid port using the `no portmode hybrid` command.

NOTE: You must remove all other configurations on the port before you can remove the hybrid configuration from the port.

Example

```
FTOS(conf)#interface te 7/0
FTOS(conf-if-te-7/0)#portmode hybrid
FTOS(conf-if-te-7/0)#interface vlan 10
FTOS(conf-if-vl-10)#untagged gi 7/0
FTOS(conf-if-vl-10)#interface vlan 20
FTOS(conf-if-vl-20)#tagged gi 7/0
FTOS(conf-if-vl-20)#
```

Example

```
FTOS(conf-if-vl-20)#do show interfaces switchport
Name: TenGigabitEthernet 7/0
802.1QTagged: Hybrid
Vlan membership:
Vlan  10,   Vlan 20
Native   VlanId: 10
FTOS(conf-if-vl-20)#
```

Example (Vlan)

```
FTOS(conf-if-vl-20)#interface vlan 10
FTOS(conf-if-vl-10)#no untagged te 7/0
FTOS(conf-if-vl-10)#interface vlan 20
FTOS(conf-if-vl-20)#no tagged te 7/0
FTOS(conf-if-vl-20)#interface te 7/0
FTOS(conf-if-te-7/0)#no portmode hybrid
FTOS(conf-if-vl-20)#
```

Related Commands

show interfaces switchport – displays the configuration of switchport (Layer 2) interfaces on the switch.

switchport – places the interface in a Layer 2 mode.

vlan-stack trunk – specifies an interface as a trunk port to the Stackable VLAN network.

rate-interval

Configure the traffic sampling interval on the selected interface.

S5000

Syntax `rate-interval seconds`

Parameters

seconds	Enter the number of seconds for which to collect traffic data. The range is 30 to 299 seconds. **NOTE:** Because polling occurs every 15 seconds, the number of seconds designated here will round to the multiple of 15 seconds lower than the entered value. For example, if 44 seconds is designated, it will round to 30; 45 to 59 seconds will round to 45, and so forth.

Defaults 299 seconds

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	The output of the `show interfaces` command displays the configured rate interval, along with the collected traffic data.
Related Commands	show interfaces – displays information on physical and virtual interfaces.

show config

Display the interface configuration.

S5000

Syntax

`show config`

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-if)#show conf
!
interface TenGigabitEthernet 0/0
 ip address 10.1.1.1/16
 portmode hybrid
 switchport
 dcb-policy input pfc3
 no shutdown
FTOS(conf-if)#
```

show config (from INTERFACE RANGE mode)

Display the bulk configured interfaces (`interface range`).

S5000

Syntax

`show config`

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-if-range-te-0/1)#interface range tengig 0/1 - 2
FTOS(conf-if-range-te-0/1-2)#show config
!
interface TenGigabitEthernet 0/1
 no ip address
 portmode hybrid
 switchport
 dcb-policy input pfc3
 no shutdown
!
interface TenGigabitEthernet 0/2
 no ip address
 portmode hybrid
 switchport
 dcb-policy input pfc3
 no shutdown
```

show interfaces

Display information on a specific physical interface or virtual interface.

S5000

Syntax `show interfaces` *`type slot/port`*

Parameters

interfaces *type slot/port*	Enter one of the following keywords and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Fibre Channel interface, enter the keyword `FibreChannel` followed by slot/port numbers. The port range is 0 to 47. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0. • For a Null interface, enter the keywords `null 0`. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `show interfaces` command for details on a specific interface. Use the `show interfaces stack-unit` command for details on all interfaces on the designated stack-unit.

On the S5000, the `show interface` output displays incorrect rate information details over time for link monitoring when the rate-interval is configured for **5 seconds**. Dell Networking recommends using higher rate-intervals such as **15** to **299 seconds** to minimize the errors seen.

NOTE: In the CLI output, the power value is rounded to a 3-digit value. For receive/transmit power that is less than 0.000, an `snmp query` returns the corresponding dbm value even though the CLI displays as 0.000.

NOTE: After the counters are cleared, the line-rate continues to increase until it reaches the maximum line rate. When the maximum line rate is reached, there is no change in the line-rate.

The following describes the `show interfaces` command shown in the Example below.

TenGigabitEthernet 0/0...	Interface type, slot/port, and administrative and line protocol status.
Hardware is...	Interface hardware information, assigned MAC address, and current address.
Pluggable media present...	Present pluggable media wavelength, type, and rate. The error scenarios are: • Wavelength, Non-qualified — Dell Networking (Force10) ID is not present, but wavelength information is available from XFP or SFP serial data • Wavelength, F10 unknown—Dell Networking (Force10) ID is present, but not able to determine the optics type • Unknown, Non-qualified— if wavelength is reading error, and F10 ID is not present Although the S5000 allows unsupported SFP and XFP transceivers to be used, but FTOS might not be able to retrieve some data about them. In that case, typically when the output of this field is “Pluggable media present, Media type is unknown”, the Medium and the XFP/SFP receive power reading data might not be present in the output.
Interface index...	Displays the interface index number used by SNMP to identify the interface.
Internet address...	States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.
MTU 1554...	Displays link and IP MTU information.
LineSpeed...	Displays the interface’s line speed, duplex mode, and slave.
Flowcontrol...	Displays receive and transmit status.
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the `show interfaces` counters where cleared.

Queuing strategy...	States the packet queuing strategy. FIFO means first in first out.
Input Statistics:	Displays all the input statistics including: • Number of packets and bytes into the interface • Number of packets with VLAN tagged headers • Packet size and the number of those packets inbound to the interface • Number of Multicast and Broadcast packets: – Multicasts = number of MAC multicast packets – Broadcasts = number of MAC broadcast packets • Number of runts, giants, and throttles packets: – runts = number of packets that are less than 64B – giants = packets that are greater than the MTU size – throttles = packets containing PAUSE frames • Number of CRC, overrun, and discarded packets: – CRC = packets with CRC/FCS errors – overrun = number of packets discarded due to FIFO overrun conditions – discarded = the sum of runts, giants, CRC, and overrun packets discarded without any processing
Output Statistics:	Displays output statistics sent out of the interface including: • Number of packets, bytes, and underruns out of the interface • Packet size and the number of those packets outbound to the interface • Number of Multicast, Broadcast, and Unicast packets: – Multicasts = number of MAC multicast packets – Broadcasts = number of MAC broadcast packets – Unicasts = number of MAC unicast packets • Number of VLANs, throttles, discards, and collisions: – Vlans = number of VLAN tagged packets – throttles = packets containing PAUSE frames – discarded = number of packets discarded without any processing – collisions = number of packet collisions – wred = count both packets discarded in the MAC and in the hardware-based queues
Rate information...	Estimate of the input and output traffic rate over a designated interval (30 to 299 seconds). Traffic rate is displayed in bits, packets per second, and percent of line rate.
Time since...	Elapsed time since the last interface status change (hh:mm:ss format).

Example (single interface)

```
FTOS#show interfaces tengigabitethernet 0/2
TenGigabitEthernet 0/2 is up, line protocol is up
Hardware is DellEth, address is 5c:f9:dd:ee:ff:c2
  Current address is 5c:f9:dd:ee:ff:c2
Pluggable media present, SFP+ type is 10GBASE-SR
  Medium is MultiRate, Wavelength is 850nm
  SFP+ receive power reading is -2.1817dBm
Interface index is 34407432
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10000 Mbit
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 3d21h48m
Queueing strategy: fifo
Input Statistics:
 0 packets, 0 bytes
 0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte
pkts
 0 Multicasts, 0 Broadcasts
 0 runts, 0 giants, 0 throttles
 0 CRC, 0 overrun, 0 discarded
Output Statistics:
 34186 packets, 3888988 bytes, 0 underruns
 2 64-byte pkts, 34188 over 64-byte pkts, 0 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte
pkts
 34190 Multicasts, 0 Broadcasts, 0 Unicasts
 0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
 Input 00.00 Mbits/sec,   0 packets/sec, 0.00% of line-rate
 Output 00.00 Mbits/sec,   0 packets/sec, 0.00% of line-rate
Time since last interface status change: 3d21h45m
```

Usage Information

The interface counter “over 1023-byte pkts” does not increment for packets in the range 9216 > x < 1023.

The Management port is enabled by default (`no shutdown`). If necessary, use the `ip address` command to assign an IP address to the Management port. If your system has more than one stack-unit, use the `show redundancy` command to display which stack-unit is the primary unit.

Example (ManagementEthernet)

```
FTOS#show interfaces managementethernet 0
ManagementEthernet 0/0 is up, line protocol is up
Hardware is DellEth, address is 5c:f9:dd:ee:ff:c2
    Current address is 5c:f9:dd:ee:ff:c2
Pluggable media not present
Interface index is 436486344
Internet address is 10.1.1.1/16
Virtual-IP is not set
Virtual-IP IPv6 address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 100 Mbit, Mode full duplex
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 3d21h47m
Queueing strategy: fifo
    Input 276762 packets, 23957349 bytes, 265199 multicast
    Received 0 errors, 0 discarded
    Output 8521 packets, 2229204 bytes, 9 multicast
    Output 0 errors, 0 invalid protocol
Time since last interface status change: 3d21h47m
```

Related Commands

show interfaces configured – displays any interface with a non-default configuration.

show interfaces stack-unit – displays information on all interfaces on a specific stack-unit.

show interfaces rate – displays information of either rate limiting or rate policing on the interface.

show interfaces switchport – displays Layer 2 information about the interfaces.

show inventory – displays the switch type, components (including media), FTOS version including hardware identification numbers, and configured protocols.

show ip interface – displays Layer 3 information about the interfaces.

show stack-unit – displays the status of the stack-unit(s).

show range – displays all interfaces configured using the interface range command.

show interfaces configured

Display any interface with a non-default configuration.

S5000

Syntax

```
show interfaces configured
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show interfaces configured
TenGigabitEthernet 0/10 is up, line protocol is up
Hardware is DellEth, address is 5c:f9:dd:ee:ff:c2
    Current address is 5c:f9:dd:ee:ff:c2
Pluggable media present, SFP+ type is 10GBASE-SR
    Medium is MultiRate, Wavelength is 850nm
    SFP+ receive power reading is -3.1158dBm
Interface index is 36242440
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10000 Mbit
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 2d23h34m
Queueing strategy: fifo
Input Statistics:
 0 packets, 0 bytes
 0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte
pkts
 0 Multicasts, 0 Broadcasts
 0 runts, 0 giants, 0 throttles
 0 CRC, 0 overrun, 0 discarded
Output Statistics:
 355 packets, 40162 bytes, 0 underruns
 0 64-byte pkts, 355 over 64-byte pkts, 0 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte
pkts
 355 Multicasts, 0 Broadcasts, 0 Unicasts
 0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
 Input 00.00 Mbits/sec,    0 packets/sec, 0.00% of line-rate
 Output 00.00 Mbits/sec,    0 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:23:23


FTOS#
```

Related Commands show interfaces – displays information on a specific physical interface or virtual interface.

show interfaces dampening

Display interface dampening information.

S5000

Syntax `show interfaces dampening [[interface-type slot/port] [summary] [detail]]`

Parameters

interface-type slot/port	(Optional) Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
summary	(OPTIONAL) Enter the keyword `summary` to display the current summary of dampening data, including the number of interfaces configured and the number of interfaces suppressed, if any.
detail	(OPTIONAL) Enter the keyword `detail` to display detailed interface dampening data.

Defaults none

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show interfaces dampening
Interface Supp   Flaps Penalty Half-Life Reuse Suppress Max-Sup
          State
Te 3/2    Up     0     0        20       800   4500     120
Te 3/10   Up     0     0        5        750   2500     20
FTOS#
```

Related Commands

dampening – configures dampening on an interface.

show interfaces – displays information on a specific physical interface or virtual interface.

show interfaces configured – displays any interface with a non-default configuration.

show interfaces description

Display the descriptions configured on the interface.

S5000

Syntax

```
show interfaces [type slot/port] description
```

Parameters

interfaces *type slot/port*

(OPTIONAL) Enter the `interfaces` keyword followed by the interface type and slot/port or number information, then enter the `description` keyword.. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below.

- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a range of interfaces, enter the keyword `range` followed by slot/port number.
- For a Fibre Channel interface, enter the keyword `FibreChannel` followed by slot/port numbers. The port range is 0 to 47.
- For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
- For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0.
- For a Null interface, enter the keywords `null 0`.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show interfaces description` command shown in the Example below.

Field	Description
Interface	Displays the type of interface and associated slot and port number.
OK?	Indicates if the hardware is functioning properly.
Status	States whether the interface is enabled (up) or disabled (administratively down).
Protocol	States whether IP is enabled (up) or disabled (down) on the interface.
Description	Displays the description (if any) manually configured for the interface.

Example

```
FTOS#show interfaces description
Interface                OK  Status     Protocol    Description
TenGigabitEthernet 0/0   YES up         up
TenGigabitEthernet 0/1   NO  admin down down
TenGigabitEthernet 0/2   NO  admin down down
TenGigabitEthernet 0/3   NO  admin down down
TenGigabitEthernet 0/4   NO  admin down down
TenGigabitEthernet 0/5   NO  admin down down
TenGigabitEthernet 0/6   YES up         up
TenGigabitEthernet 0/7   YES up         up
TenGigabitEthernet 0/8   NO  admin down down
TenGigabitEthernet 0/9   NO  admin down down
TenGigabitEthernet 0/10  NO  up         down
TenGigabitEthernet 0/11  YES up         up
TenGigabitEthernet 0/24  NO  admin down down
TenGigabitEthernet 0/25  NO  admin down down
TenGigabitEthernet 0/26  YES up         up
TenGigabitEthernet 0/27  YES up         up
TenGigabitEthernet 0/28  YES up         up
TenGigabitEthernet 0/29  YES up         up
TenGigabitEthernet 0/30  NO  admin down down
TenGigabitEthernet 0/31  NO  admin down down
TenGigabitEthernet 0/32  NO  admin down down
TenGigabitEthernet 0/33  NO  admin down down
TenGigabitEthernet 0/34  NO  admin down down
TenGigabitEthernet 0/35  NO  admin down down
fortyGigE 0/48           NO  admin down down
fortyGigE 0/52           NO  admin down down
fortyGigE 0/56           NO  admin down down
fortyGigE 0/60           NO  admin down down
ManagementEthernet 0/0   YES up         up
ManagementEthernet 1/0   NO  up         not present
ManagementEthernet 2/0   NO  up         not present
ManagementEthernet 3/0   NO  up         not present
ManagementEthernet 4/0   NO  up         not present
ManagementEthernet 5/0   NO  up         not present
ManagementEthernet 6/0   NO  up         not present
ManagementEthernet 7/0   NO  up         not present
ManagementEthernet 8/0   NO  up          not present
ManagementEthernet 9/0   NO  up          not present
ManagementEthernet 10/0  NO  up          not present
ManagementEthernet 11/0  NO  up          not present
Vlan 1                   NO  admin down down
Vlan 100                 NO  admin down down
FTOS#
```

Related Commands

show interfaces – displays information on a specific physical interface or virtual interface.

show interfaces stack-unit

Display information on all interfaces on a specific S5000 stack member.

S5000

Syntax

`show interfaces stack-unit` *`unit-number`*

Parameters

stack-unit *unit-number*	Enter the keyword `stack-unit` followed by the unit number. The range is 0 to 11.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#sh int stack-unit 0
TenGigabitEthernet 0/0 is up, line protocol is up
Hardware is DellEth, address is 5c:f9:dd:ee:ff:c2
   Current address is 5c:f9:dd:ee:ff:c2
Pluggable media present, SFP+ type is 10GBASE-SR
   Medium is MultiRate, Wavelength is 850nm
   SFP+ receive power reading is -2.4018dBm
Interface index is 33883144
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10000 Mbit
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 3d22h23m
Queueing strategy: fifo
Input Statistics:
 0 packets, 0 bytes
 0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte
pkts
 0 Multicasts, 0 Broadcasts
 0 runts, 0 giants, 0 throttles
 0 CRC, 0 overrun, 0 discarded
Output Statistics:
 29704 packets, 3333165 bytes, 0 underruns
 2 64-byte pkts, 29705 over 64-byte pkts, 0 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte
pkts
 29707 Multicasts, 0 Broadcasts, 0 Unicasts
 0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
 Input 00.00 Mbits/sec,     0 packets/sec, 0.00% of line-rate
 Output 00.00 Mbits/sec,     0 packets/sec, 0.00% of line-rate
Time since last interface status change: 3d22h19m

TenGigabitEthernet 0/1 is down, line protocol is down
Hardware is DellForce10Eth, address is 5c:f9:dd:ee:ff:c2
    Current address is 5c:f9:dd:ee:ff:c2
Pluggable media present, SFP+ type is 10GBASE-SR
  Medium is MultiRate, Wavelength is 850nm
  No power
Interface index is 33883144
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 2d23h41m

!-----------------output truncated ----------------!
```

Related Commands

show hardware stack-unit – displays data plane and management plane input/output statistics.

show interfaces – displays information on a specific physical interface or virtual interface.

show interfaces status

Display a summary of interface information or specify a stack-unit and interface to display status information on that specific interface only.

S5000

Syntax

`show interfaces [type slot/port] status`

Parameters

interfaces *type slot/port*	(OPTIONAL) Enter the `interfaces` keyword followed by the interface type and slot/port or number information, then enter the `status` keyword.. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a range of interfaces, enter the keyword `range` followed by slot/port number.

- For a Fibre Channel interface, enter the keyword `FibreChannel` followed by slot/port numbers. The port range is 0 to 47.
- For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
- For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0.
- For a Null interface, enter the keywords `null 0`.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults	none
Command Modes	• EXEC • EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
FTOS#show interfaces status
Port    Description  Status Speed      Duplex Vlan
Te 0/0               Up     10000 Mbit Full   --
Te 0/1               Down   Auto       Auto   --
Te 0/2               Down   Auto       Auto   --
Te 0/3               Down   Auto       Auto   --
Te 0/4               Down   Auto       Auto   --
Te 0/5               Down   Auto       Auto   --
Te 0/6               Up     10000 Mbit Full   100
Te 0/7               Up     10000 Mbit Full   --
Te 0/8               Down   Auto       Auto   --
Te 0/9               Down   Auto       Auto   --
Te 0/10              Down   Auto       Auto   --
Te 0/11              Up     10000 Mbit Full   100
Te 0/24              Down   Auto       Auto   --
Te 0/25              Down   Auto       Auto   --
Te 0/26              Up     10000 Mbit Full   --
Te 0/27              Up     10000 Mbit Full   --
Te 0/28              Up     10000 Mbit Full   --
Te 0/29              Up     10000 Mbit Full   --
Te 0/30              Down   Auto       Auto   --
Te 0/31              Down   Auto       Auto   --
Te 0/32              Down   Auto       Auto   --
Te 0/33              Down   Auto       Auto   --
Te 0/34              Down   Auto       Auto   --
Te 0/35              Down   Auto       Auto   --
Fo 0/48              Down   40000 Mbit Auto   --
Fo 0/52              Down   40000 Mbit Auto   --
Fo 0/56              Down   40000 Mbit Auto   --
Fo 0/60              Down   40000 Mbit Auto   --
FTOS#
```

Related Commands	show interfaces – displays information on a specific physical interface or virtual interface.

show interfaces switchport

Display only virtual and physical interfaces in Layer 2 mode. This command displays the Layer 2 mode interfaces' IEEE 802.1Q tag status and VLAN membership.

S5000

Syntax

```
show interfaces switchport [interface-type slot/port ] | backup
| stack-unit unit-number ]
```

Parameters

interface-type slot/port	(OPTIONAL) Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
backup	Enter the keyword `backup` to view the backup interface for this interface.
stack-unit *unit-number*	Enter the keyword `stack-unit` followed by the unit number. The range is 0 to 11.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show interfaces switchport` command for the Example below.

Name	Displays the interface's type, slot, and port number.
802.1QTagged	Displays whether if the VLAN tagged ("True"), untagged ("False"), or hybrid ("Hybrid"), which supports both untagged and tagged VLANs by port 13/0.
Vlan membership	Lists the VLANs to which the interface is a member. This field can display native VLAN membership by port 13/0.

Example

```
FTOS#show interfaces switchport
Name: TenGigabitEthernet 13/0
802.1QTagged: Hybrid
Vlan membership:
Vlan   2, Vlan 20
Native VlanId: 20

Name: TenGigabitEthernet 13/1
802.1QTagged: True
Vlan membership:
Vlan   2

Name: TenGigabitEthernet 13/2
802.1QTagged: True
Vlan membership:
Vlan   2

Name: TenGigabitEthernet 13/3
802.1QTagged: True
Vlan membership:
Vlan   2
--More--
```

Related Commands

interface – configures a physical interface on the switch.

show ip interface – displays Layer 3 information about the interfaces.

show interfaces – displays information on a specific physical interface or virtual interface.

show interfaces transceiver – displays the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

show interfaces transceiver

Display the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

S5000

Syntax

```
show interfaces [tengigabitethernet slot/port | fortyGigE slot/
port] transceiver
```

Parameters

tengigabitethernet	For a 10G interface, enter the keyword `tengigabitethernet` followed by the slot/port information.
fortyGigE	For a 40G interface, enter the keyword `fortyGigE` followed by the slot/port information.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show interfaces transceiver` command output shown in the Example below.

Table 5. Output Fields for the **`show interfaces transceiver`** Command

Field	Description
Rx Power measurement type	Output depends on the vendor, typically either “Average” or “OMA” (Receiver optical modulation amplitude).
Temp High Alarm threshold	Factory-defined setting, typically in Centigrade. Value differs between SFPs and SFP+.
Voltage High Alarm threshold	Displays the interface index number used by SNMP to identify the interface.
Bias High Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power High Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
RX Power High Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temp Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Voltage Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Bias Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
RX Power Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temp High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Voltage High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Bias High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
RX Power High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.

Field	Description
Temp Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Voltage Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Bias Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Power Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temperature	Current temperature of the SFPs. If this temperature crosses Temp High alarm/warning thresholds, the temperature high alarm/warning flag is set to true.
Voltage	Current voltage of the SFPs. If this voltage crosses voltage high alarm/warning thresholds, the voltage high alarm/warning flag is set to true.
Tx Bias Current	Present Tx bias current of the SFP. If this crosses bias high alarm/warning thresholds, the Tx bias high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, the Tx bias low alarm/warning flag is set to true.
Tx Power	Present Tx power of the SFP. If this crosses Tx power alarm/warning thresholds, the Tx power high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, the Tx power low alarm/warning flag is set to true.
Rx Power	Present Rx power of the SFP. This value is either average Rx power or OMA. This depends on the Rx Power measurement type displayed above. If this crosses Rx power alarm/warning thresholds, the Rx power high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, the Rx power low alarm/warning flag is set to true.
Data Ready state Bar	This field indicates that the transceiver has achieved power up and data is ready. This is set to true if data is ready to be sent and set to false if data is being transmitted.
Rx LOS state	This is the digital state of the Rx_LOS output pin. This is set to true if the operating status is down.
Tx Fault state	This is the digital state of the Tx Fault output pin.
Rate Select state	This is the digital state of the SFP rate_select input pin.

Field	Description
RS state	This is the reserved digital state of the pin AS(1) per SFF-8079 and RS(1) per SFF-8431.
Tx Disable state	If the admin status of the port is down then this flag is set to true.
Temperature High Alarm Flag	This can be either true or false, depending on the Current voltage value displayed above.
Voltage High Alarm Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Tx Bias High Alarm Flag	This can be either true or false, depending on the present Tx bias current value displayed above.
Tx Power High Alarm Flag	This can be either true or false, depending on the Current Tx bias power value displayed above.
Rx Power High Alarm Flag	This can be either true or false, depending on the Current Rx power value displayed above.
Temperature Low Alarm Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Voltage Low Alarm Flag	This can be either true or false, depending on the Current voltage value displayed above.
Tx Bias Low Alarm Flag	This can be either true or false, depending on the Tx bias current value displayed above.
Tx Power Low Alarm Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power Low Alarm Flag	This can be either true or false, depending on the Current Rx power value displayed above.
Temperature High Warning Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Voltage High Warning Flag	This can be either true or false, depending on the Current voltage value displayed above.
Tx Bias High Warning Flag	This can be either true or false, depending on the Tx bias current value displayed above.
Tx Power High Warning Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power High Warning Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Temperature Low Warning Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Voltage Low Warning Flag	This can be either true or false, depending on the Current voltage value displayed above.

Field	Description
Tx Bias Low Warning Flag	This can be either true or false, depending on the present Tx bias current value displayed above.
Tx Power Low Warning Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power Low Warning Flag	This can be either true or false, depending on the Current Rx power value displayed above.

Example

```
FTOS#show interfaces tengigabitethernet 1/0 transceiver
SFP is present.

SFP 0 Serial Base ID fields
SFP 0 Id                 = 0x03
SFP 0 Ext Id             = 0x04
SFP 0 Connector          = 0x07
SFP 0 Transciever Code = 0x00 0x00 0x00 0x01 0x20 0x40 0x0c
0x05
SFP 0 Encoding           = 0x01
SFP 0 BR Nominal         = 0x15
SFP 0 Length(9um) Km     = 0x00
SFP 0 Length(9um) 100m   = 0x00
SFP 0 Length(50um) 10m   = 0x1e
SFP 0 Length(62.5um) 10m  = 0x0f
SFP 0 Length(Copper) 10m  = 0x00
SFP 0 Vendor Rev         = A
SFP 0 Laser Wavelength   = 850 nm
SFP 0 CheckCodeBase      = 0x66
SFP 0 Serial Extended ID fields
SFP 0 Options            = 0x00 0x12
SFP 0 BR max= 0
SFP 0 BR min= 0
SFP 0 Vendor SN= P5N1ACE
SFP 0 Datecode           = 040528
SFP 0 CheckCodeExt       = 0x5b

SFP 1 Diagnostic Information
===================================
SFP 1 Rx Power measurement type     = Average
===================================
SFP 1 Temp High Alarm threshold       = 95.000C
SFP 1 Voltage High Alarm threshold    = 3.900V
SFP 1 Bias High Alarm threshold       = 17.000mA
SFP 1 TX Power High Alarm threshold   = 0.631mW
SFP 1 RX Power High Alarm threshold   = 1.259mW
SFP 1 Temp Low Alarm threshold        = -25.000C
SFP 1 Voltage Low Alarm threshold     = 2.700V
SFP 1 Bias Low Alarm threshold        = 1.000mA
SFP 1 TX Power Low Alarm threshold    = 0.067mW
SFP 1 RX Power Low Alarm threshold    = 0.010mW
===================================
SFP 1 Temp High Warning threshold     = 90.000C
SFP 1 Voltage High Warning threshold  = 3.700V
SFP 1 Bias High Warning threshold     = 14.000mA
SFP 1 TX Power High Warning threshold = 0.631mW
SFP 1 RX Power High Warning threshold = 0.794mW
SFP 1 Temp Low Warning threshold      = -20.000C
SFP 1 Voltage Low Warning threshold   = 2.900V
SFP 1 Bias Low Warning threshold      = 2.000mA
SFP 1 TX Power Low Warning threshold  = 0.079mW
SFP 1 RX Power Low Warning threshold  = 0.016mW
===================================
SFP 1 Temperature                     = 39.930C
SFP 1 Voltage                         = 3.293V
SFP 1 Tx Bias Current                 = 6.894mA
SFP 1 Tx Power                        = 0.328mW
SFP 1 Rx Power                        = 0.000mW
===================================
SFP 1 Data Ready state Bar            = False
SFP 1 Rx LOS state                    = True
SFP 1 Tx Fault state                  = False
SFP 1 Rate Select state               = False
SFP 1 RS state                        = False
SFP 1 Tx Disable state                = False
===================================
SFP 1 Temperature High Alarm Flag     = False
SFP 1 Voltage High Alarm Flag         = False
SFP 1 Tx Bias High Alarm Flag         = False
SFP 1 Tx Power High Alarm Flag        = False
SFP 1 Rx Power High Alarm Flag        = False
SFP 1 Temperature Low Alarm Flag      = False
SFP 1 Voltage Low Alarm Flag          = False
SFP 1 Tx Bias Low Alarm Flag          = False
SFP 1 Tx Power Low Alarm Flag         = False
SFP 1 Rx Power Low Alarm Flag         = True
===================================
!-------output truncated -------------------------!
```

Related Commands

interface – configures a physical interface on the switch.

show ip interface – displays Layer 3 information about the interfaces.

show interfaces – displays information on a specific physical interface or virtual interface.

show inventory – displays the S5000 switch components (including media), FTOS version including hardware identification numbers, and configured protocols.

show range

Display all interfaces configured using the `interface range` command.

S5000

Syntax

```
show range
```

Command Modes

INTERFACE RANGE (config-if-range)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-if-range-so-2/0-1,fa-0/0)#show range
interface tengigabitethernet 2/0 - 1
interface tengigabitethernet 0/0
FTOS(conf-if-range-so-2/0-1,fa-0/0)#
```

Related Commands	interface – configures a physical interface on the switch. show ip interface – displays Layer 3 information about the interfaces. show interfaces – displays information on a specific physical interface or virtual interface.

show running-config ecmp-group

Display interfaces, LAG, or LAG link bundles being monitored for uneven traffic distribution using the `ecmp-group monitoring enable` command. The ECMP group could have a LAG or a list of 10G/40 interfaces (not just LAG link-bundles).

S5000

Syntax `show running-config ecmp-group`

Defaults Disabled.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands ecmp-group – configures a mechanism to monitor traffic distribution.

shutdown

Disable an interface.

S5000

Syntax `shutdown`

To activate an interface, use the `no shutdown` command.

Defaults The interface is disabled.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `shutdown` command marks a physical interface as unavailable for traffic. To discover if an interface is disabled, use the `show ip interface brief` command. Disabled interfaces are listed as down.

Disabling a VLAN or a port channel causes different behavior. When a VLAN is disabled, the Layer 3 functions within that VLAN are disabled. Layer 2 traffic continues to flow. Entering the `shutdown` command on a port channel disables all traffic on the port channel and the individual interfaces within the port channel. To enable a port channel, you must enter `no shutdown` on the port channel interface and at least one interface within that port channel.

The `shutdown` and `description` commands are the only commands that you can configure on an interface that is a member of a port channel.

Related Commands	interface port-channel – creates a port channel interface. interface vlan – creates a VLAN. show ip interface – displays the interface routing status. Add the keyword `brief` to display a table of interfaces and their status.

speed (Management interface)

Set the speed for a Management interface.

S5000

Syntax

`speed {10 | 100 | 10000 | auto}`

To return to the default setting, use the `no speed {10 | 100}` command.

Parameters

10	Enter the keyword `10` to set the interface’s speed to 10 Mb/s.
100	Enter the keyword `100` to set the interface’s speed to 10/100 Mb/s.
10000	Enter the keyword `10000` to set the interface’s speed to 1000 Mb/s (1 Gb/s).
auto	Enter the keyword `auto` to set the interface to auto-negotiate its speed.

Defaults auto

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This command is supported only on a Management interface.

Related Commands

interface ManagementEthernet – configures the Management port on the system (either the primary or standby stack-unit).

duplex (10/100 Interfaces) – configures duplex mode on physical interfaces with the speed set to 10/100.

management route – configures a static route that points to the Management interface or a forwarding router.

stack-unit portmode

Split a single 40G port into 4-10G ports on the S5000.

S5000

Syntax	`stack-unit` *`unit-number`* `port` *`number`* `portmode quad`
Parameters	**stack-unit** ***unit-number*** — Enter the keyword `stack-unit` followed by the unit number to reset. The range is 0 to 11. **port** ***number*** — Enter the keyword `port` followed by the number of the 40G port to be split. The ports are 48, 52, 56, or 60.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

Usage Information

Splitting a 40G port into 4x10G port is supported only on a standalone unit.

- Split ports cannot be used as stack-link to stack an S5000.
- Split ports on the S5000 cannot be a part of any stacked system.
- The unit number with the split ports must be the default (stack-unit 0).
- This can be verified using CLI `show system brief`. If the unit ID is different than 0, it must be renumbered to 0 before ports are split by using the `stackunit id renumber 0` command in EXEC mode.

The quad port must be in a default configuration before it can be split into 4x10G ports. The 40G port is lost in the config when the port is split, so be sure the port is also removed from other L2/L3 feature configurations.

The system must be reloaded after issuing the CLI for the change to take effect.

switchport

Place an interface in Layer 2 mode.

S5000

Syntax

`switchport [backup interface {gigabit` *`slot/port`* `| tengigabit` *`slot/port`* `| fortyGigE` *`slot/port`* `| port-channel` *`number`*`}]`

To remove an interface from Layer 2 mode and place it in Layer 3 mode, enter the `no switchport` command. If a switchport backup interface is configured, you must first remove the backup configuration. To remove a switchport backup interface, enter the `no switchport backup interface {gigabit slot/port | tengigabit slot/port | fortyGigE slot/port | port-channel number}` command.

Parameters

backup interface	Use this option to configure a redundant Layer 2 link without using Spanning Tree. The keywords `backup interface` configures a backup port so that if the primary port fails, the backup port changes to the up state. If the primary later comes up, it becomes the backup.
gigabit	Enter the keyword `gigabit` if the backup port is a 1G port.
tengigabit	Enter the keyword `tengigabit` if the backup port is a 10G port.
fortyGigE	Enter the keyword `fortyGigE` if the backup port is a 40G port.
port-channel	Enter the keywords `port-channel` if the backup port is a static or dynamic port channel.
slot/port	Specify the switch-unit and port number of the backup port.

Defaults Disabled (The interface is in Layer 3 mode.)

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If an IP address or VRRP group is assigned to the interface, you cannot use the `switchport` command on the interface. To use the `switchport` command on an interface, only the `no ip address` and `no shutdown statements` must be listed in the `show config` output.

When you enter the `switchport` command, the interface is automatically added to the default VLAN.

To use the `switchport backup interface` command on a port, you must first enter the `switchport` command. For more information, refer to the “Configuring Redundant Links” section in the “Layer 2” chapter of the *FTOS Configuration Guide*.

Related Commands

interface port-channel – creates a port channel interface.

show interfaces switchport – displays information about switchport interfaces.

Port Channel Commands

A Link Aggregation Group (LAG) is a group of links that appear to a MAC client as if they were a single link according to IEEE 802.3ad. In FTOS, a LAG is referred to as a Port Channel.

Because each port can be assigned to only one Port Channel, and each Port Channel must have at least one port, some of those nominally available Port Channels might have no function because they could have no members if there are not enough ports installed. In the S5000, those ports could be provided by stack members.

For the S5000, the maximum port channel ID is 128 and the maximum members per port channel is 8.

NOTE: The FTOS implementation of LAG or Port Channel requires that you configure a LAG on both switches manually. For information about FTOS link aggregation control protocol (LACP) for dynamic LAGs, refer to the Link Aggregation Control Protocol (LACP) chapter. For more information about configuring and using Port Channels, refer to the *FTOS Configuration Guide*.

channel-member

Add an interface to the Port Channel, while in INTERFACE PORTCHANNEL mode.

S5000

Syntax

`channel-member` *`interface-type slot/port`*

To remove an interface from a Port Channel, use the `no channel-member interface` command.

Parameters

interface-type slot/port	(OPTIONAL) Enter any of the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

Defaults

Not configured.

Command Modes

INTERFACE PORTCHANNEL

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `interface port-channel` command to access this command.

You cannot add an interface to a Port Channel if the interface contains an IP address in its configuration. Only the `shutdown`, `description`, `mtu`, and `ip mtu` commands can be configured on an interface if it is to be added to a Port Channel. The `mtu` and `ip mtu` commands are only available when the chassis is in Jumbo mode.

Link MTU and IP MTU considerations for Port Channels are:

- All members must have the same link MTU value and the same IP MTU value.
- The Port Channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members. For example, if the members have a link MTU of 2100 and an IP MTU 2000, the Port Channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

When an interface is removed from a Port Channel with the `no channel-member` command, the interface reverts to its configuration prior to joining the Port Channel.

An interface can belong to only one Port Channel.

On the S5000, you can have eight interfaces per Port Channel. The interfaces can be located on different stack-units but must be the same physical type and speed (for example, all 1-Gigabit Ethernet interfaces). However, you can combine 100/1000 interfaces and GE interfaces in the same Port Channel.

Related Commands

description – assigns a descriptive text string to the interface.

interface port-channel – creates a Port Channel interface.

shutdown – disables/enables the port channel.

group

Group two LAGs in a supergroup (“fate-sharing group” or “failover group”).

S5000

Syntax

`group group_number port-channel number port-channel number`

To remove an existing LAG supergroup, use the `no group group_number` command.

Parameters

group_number	Enter an integer from 1 to 32 that uniquely identifies this LAG fate-sharing group.
port-channel *number*	Enter the keywords `port-channel` followed by an existing LAG number. Enter this keyword/variable combination twice, identifying the two LAGs to be paired.

Defaults

none

Command Modes

PORT-CHANNEL FAILOVER-GROUP (conf-po-failover-grp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

port-channel failover-group – accesses PORT-CHANNEL FAILOVER-GROUP mode to configure a LAG failover group.

show interfaces port-channel – displays information on configured Port Channel groups.

interface port-channel

Create a Port Channel interface, which is a link aggregation group (LAG) containing up to 16 physical interfaces on the S5000 switch.

S5000

Syntax

`interface port-channel channel-number`

To delete a Port Channel, use the `no interface port-channel channel-number` command.

Parameters

channel-number	For a Port Channel interface, enter the keywords `port-channel` followed by a number. The range is 1 to 128.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Port Channel interfaces are logical interfaces and can be either in Layer 2 mode (by using the `switchport` command) or Layer 3 mode (by configuring an IP address). You can add a Port Channel in Layer 2 mode to a VLAN.

The `shutdown`, `description`, and `name` commands are the only commands that you can configure on an interface while it is a member of a Port Channel. To add a physical interface to a Port Channel, the interface can only have the `shutdown`, `description`, and `name` commands configured. The Port Channel's configuration is applied to the interfaces within the Port Channel.

A Port Channel can contain both 100/1000 interfaces and GE interfaces. Based on the first interface configured in the Port Channel and enabled, FTOS determines if the Port Channel uses 100 Mb/s or 1000 Mb/s as the common speed. For more information, refer to channel-member.

Example

```
FTOS(conf)#int port-channel 2
FTOS(conf-if-po-2)#
```

Related Commands

channel-member – adds a physical interface to the LAG.

interface – configures a physical interface.

interface loopback – configures a Loopback interface.

interface null – configures a null interface.

interface vlan – configures a VLAN.

shutdown – disables/enables the port channel.

minimum-links

Configure the minimum number of links in a LAG (Port Channel) that must be in "oper up" status for the LAG to be also in "oper up" status.

S5000

Syntax `minimum-links number`

Parameters

number	Enter the number of links in a LAG that must be in "oper up" status. The range is 1 to 16. The default is **1**.

Defaults 1

Command Modes INTERFACE

Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	If you use this command to configure the minimum number of links in a LAG that must be in “oper up” status, the LAG must have at least that number of “oper up” links before it can be declared as up. For example, if the required minimum is four, and only three are up, the LAG is considered down.

port-channel failover-group

Access PORT-CHANNEL FAILOVER-GROUP mode to configure a LAG failover group.

S5000

Syntax	`port-channel failover-group` To remove all LAG failover groups, use the `no port-channel failover-group` command.
Defaults	none
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	This feature groups two LAGs to work in tandem as a supergroup. For example, if one LAG goes down, the other LAG is taken down automatically, providing an alternate path to reroute traffic, avoiding oversubscription on the other LAG. You can use both static and dynamic (LACP) LAGs to configure failover groups. For more information, refer to the “Port Channel” chapter in the *FTOS Configuration Guide*.
Related Command	group – groups two LAGs in a supergroup (“fate-sharing group”). show interfaces port-channel – displays information on configured Port Channel groups.

show config

Display the current configuration of the selected LAG.

S5000

Syntax	`show config`
Command Modes	INTERFACE PORTCHANNEL

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-if-po-1)#show config
!
interface Port-channel 1
  no ip address
  shutdown
FTOS(conf-if-po-1)#
```

show interfaces port-channel

Display information on configured Port Channel groups.

S5000

Syntax `show interfaces port-channel [channel-number] [brief]`

Parameters

port-channel ***channel-number***	Enter the keyword `port-channel` followed by a number. The range is 1 to 128.
brief	(OPTIONAL) Enter the keyword `brief` to display only the port channel number, the state of the port channel, and the number of interfaces in the port channel.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show interfaces port-channel` command shown in the Example below.

Field	Description
Port-Channel 1...	Displays the LAG's status. In the Example, the status of the LAG's LAG fate-sharing group ("Failover-group") is listed.
Hardware is...	Displays the interface's hardware information and its assigned MAC address.
Port-channel is part...	Indicates whether the LAG is part of a LAG fate-sharing group ("Failover-group").
Internet address...	States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.
MTU 1554...	Displays link and IP MTU.

LineSpeed	Displays the interface's line speed. For a port channel interface, it is the line speed of the interfaces in the port channel.
Members in this...	Displays the interfaces belonging to this port channel.
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the `show interfaces` counters were cleared.
Queueing strategy.	States the packet queuing strategy. FIFO means first in first out.
packets input...	Displays the number of packets and bytes into the interface.
Input 0 IP packets...	Displays the number of packets with IP headers, VLAN tagged headers, and MPLS headers. The number of packets may not add correctly because a VLAN tagged IP packet counts as both a VLAN packet and an IP packet.
0 64-byte...	Displays the size of packets and the number of those packets entering that interface. This information is displayed over two lines.
Received 0...	Displays the type and number of errors or other specific packets received. This information is displayed over three lines.
Output 0...	Displays the type and number of packets sent out the interface. This information is displayed over three lines.
Rate information...	Displays the traffic rate information into and out of the interface. Traffic rate is displayed in bits and packets per second.
Time since...	Displays the time since the last change in the configuration of this interface.

Example

```
FTOS#show interfaces port-channel 20
Port-channel 20 is up, line protocol is up (Failover-group 1
is down)
Hardware address is 00:01:e8:01:46:fa
Port-channel is part of failover-group 1
Internet address is 1.1.120.1/24
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 2000 Mbit
Members in this channel: Te 0/5 Te 0/18
ARP type: ARPA, ARP timeout 04:00:00
Last clearing of "show interfaces" counters 00:00:00
Queueing strategy: fifo
  44507301 packets input, 3563070343 bytes
  Input 44506754 IP Packets, 0 Vlans 0 MPLS
  41 64-byte pkts, 44502871 over 64-byte pkts, 249 over 127-
byte pkts
  407 over 255-byte pkts, 3127 over 511-byte pkts, 606 over
1023-byte pkts
  Received 0 input symbol errors, 0 runts, 0 giants, 0
throttles
  0 CRC, 0 IP Checksum, 0 overrun, 0 discarded
  1218120 packets output, 100745130 bytes, 0 underruns
  Output 5428 Multicasts, 4 Broadcasts, 1212688 Unicasts
  1216142 IP Packets, 0 Vlans, 0 MPLS
  0 throttles, 0 discarded
Rate info (interval 299 sec):
  Input 01.50Mbits/sec, 2433 packets/sec
  Output 00.02Mbits/sec,4 packets/sec
Time since last interface status change: 00:22:34

FTOS#
```

Usage Information

The following describes the `show interfaces port-channel brief` command shown in the Example below.

Field	Description
LAG	Lists the port channel number.
Mode	Lists the mode: • L3 - for Layer 3 • L2 - for Layer 2
Status	Displays the status of the port channel. • down - if the port channel is disabled (`shutdown`) • up - if the port channel is enabled (`no shutdown`)
Uptime	Displays the age of the port channel in hours:minutes:seconds.
Ports	Lists the interfaces assigned to this port channel.
(untitled)	Displays the status of the physical interfaces (up or down). • In Layer 2 port channels, an * (asterisk) indicates which interface is the primary port of the port channel. The primary port sends out interface PDU. • In Layer 3 port channels, the primary port is not indicated.

Example

```
FTOS#sh int por 1 br

LAG Mode Status Uptime    Ports
1   L2   up     00:00:08  Te 3/0 (Up) *
                          Te 3/1 (Down)
                          Te 3/2 (Up)
FTOS#
```

Related Commands

show lacp – displays the LACP matrix.

show port-channel-flow

Display an egress port in a given port-channel flow.

S5000

Syntax

```
show port-channel-flow outgoing-port-channel number incoming-
interface interface {source-ip address destination-ip address}
| {source-port number destination-port number} | {source-mac
address destination-mac address}
```

Parameters

outgoing-port-channel *number*	Enter the keywords `outgoing-port-channel` followed by the number of the port channel to display flow information. For a Port Channel interface, enter the keywords `port-channel` followed by a number. The range is 1 to 128.
incoming-interface *interface*	Enter the keywords `incoming-interface` followed by the interface type and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
source-ip *address*	Enter the keywords `source-ip` followed by the IP source address in IP address format.
destination-ip *address*	Enter the keywords `destination-ip` followed by the IP destination address in IP address format.
source-port *number*	Enter the keywords `source-port` followed by the source port number. The range is 1 to 65536. The default is **None**.
destination-port *number*	Enter the keywords `destination-port` followed by the destination port number. The range is 1 to 65536. The default is **None**.
source-mac *address*	Enter the keywords `source-mac` followed by the MAC source address in the nn:nn:nn:nn:nn:nn format.
destination-mac *address*	Enter the keywords `destination-mac` followed by the MAC destination address in the nn:nn:nn:nn:nn:nn format.

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Because this command calculates based on a Layer 2 hash algorithm, use this command to display flows for switched Layer 2 packets, not for routed packets (use the `show ip flow` command to display routed packets).

The `show port-channel-flow` command returns the egress port identification in a given port-channel if a valid flow is entered. A mismatched flow error occurs if MAC-based hashing is configured for a Layer 2 interface and you are trying to display a Layer 3 flow.

The output displays three entries:

- Egress port for unfragmented packets.
- In the event of fragmented packets, the egress port of the first fragment.
- In the event of fragmented packets, the egress port of the subsequent fragments.

NOTE: In the `show port channel flow` command output, the egress port for an unknown unicast, multicast, or broadcast traffic is not displayed.

The Example below shows the `show port-channel-flow outgoing-port-channel` *`number`* `incoming-interface` *`interface`* `source-mac` *`address`* `destination-mac` *`address`*

- Load-balance is configured for MAC
- Load-balance is configured for IP 4-tuple/2-tuple for the S5000.
- A non-IP payload is going out of Layer 2 LAG interface that is a member of VLAN with an IP address

Example

```
FTOS#show port-channel-flow outgoing-port-channel 1 incoming-
interface gi 3/0
source-mac 00:00:50:00:00:00 destination-mac 00:00:a0:00:00:00

    Egress Port for port-channel 1, for the given flow, is Te
13/01
```

Example

```
FTOS#show port-channel-flow outgoing-port-channel 2 incoming-
interface te
3/0 source-ip 2.2.2.0 destination-ip 3.2.3.1 protocol tcp
source-port 5
destination-port 6
```

Egress Port for port-channel 2, for the given flow:
Unfragmented packet: Te 1/6
Fragmented packets (first fragment): Te 1/12
Fragmented packets (remaining fragments): Te 1/12

UDP Broadcast

The user datagram protocol (UDP) broadcast feature is a software-based method to forward low throughput (not to exceed 200 pps) IP/UDP broadcast traffic arriving on a physical or VLAN interface.

Important Points to Remember

- This feature is available on the S5000 switch.
- Routing information protocol (RIP) is not supported with the UDP Broadcast feature.
- If you configure this feature on an interface using the `ip udp-helper udp-port` command, the `ip directed-broadcast` command becomes ineffective on that interface.

- The existing `show interface` command has been modified to display the configured broadcast address.

debug ip udp-helper

Enable UDP debug and display the debug information on a console.

S5000

Syntax	`debug ip udp-helper` To disable debug information, use the `no debug ip udp-helper` command.
Defaults	Debug disabled.
Command Modes	• EXEC • EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
FTOS#debug ip udp-helper
UDP helper debugging is on

01:20:22: Pkt rcvd on Te 5/0 with IP DA (0xffffffff) will be
sent on Te 5/1 Te 5/2
Vlan 3

01:44:54: Pkt rcvd on Te 7/0 is handed over for DHCP
processing.
```

Related Commands

ip udp-broadcast-address – configures a UDP IP address for broadcast.

ip udp-helper udp-port – enables the UDP broadcast feature on an interface.

show ip udp-helper – displays the configured UDP helper(s) on all interfaces.

ip udp-broadcast-address

Configure an IP UDP address for broadcast.

S5000

Syntax	`ip udp-broadcast-address` *`address`* To delete the configuration, use the `no ip udp-broadcast-address` *`address`* command.
Parameters	***address*** Enter an IP broadcast address in dotted decimal format (A.B.C.D).

Defaults

Not configured.

Command Modes

INTERFACE (config-if)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When a UDP broadcast packet is flooded out of an interface, and the outgoing interface is configured using this command, the outgoing packet's IP destination address is replaced with the configured broadcast address.

Related Commands

debug ip udp-helper – enables debug and displays the debug information on a console.

show ip udp-helper – displays the configured UDP helper(s) on all interfaces.

ip udp-helper udp-port

Enable the UDP broadcast feature on an interface either for all UDP ports or a specified list of UDP ports.

S5000

Syntax

`ip udp-helper udp-port [`*`udp-port-list`*`]`

To disable the UDP broadcast on a port, use the `no ip udp-helper udp-port [`*`udp-port-list`*`]` command.

Parameters

udp-port-list	(OPTIONAL) Enter up to 16 comma-separated UDP port numbers. **NOTE:** If you do not use this option, all UDP ports are considered by default.

Defaults

none

Command Modes

INTERFACE (config-if)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you configure the `ip helper-address` command and `ip udp-helper udp-port` command, the behavior is that the UDP broadcast traffic with port numbers 67/68 is unicast relayed to the DHCP server per the `ip helper-address` configuration. This occurs regardless if the `ip udp-helper udp-port` command contains port numbers 67/68 or not.

If you only configure the `ip udp-helper udp-port` command, all the UDP broadcast traffic is flooded, including ports 67/68 traffic if those ports are part of the `udp-port-list`.

Related Commands

ip helper-address – configures the destination broadcast or host address for the DHCP server.

debug ip udp-helper – enables debug and displays the debug information on a console.

show ip udp-helper – displays the configured UDP helper(s) on all interfaces.

show ip udp-helper

Display the configured UDP helper(s) on all interfaces.

S5000

Syntax `show ip udp-helper`

Defaults none

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip udp-helper
--------------------------------------------------
Port      UDP  port  list
--------------------------------------------------
Te 10/0  656, 658
Te 10/1  All
```

Related Commands

debug ip udp-helper – enables debug and displays the debug information on a console.

ip udp-broadcast-address – configures a UDP IP address for broadcast.

ip udp-helper udp-port – enables the UDP broadcast feature on an interface either for all UDP ports or a specified list of UDP ports.

Fibre Channel Interface Commands

The following commands are supported for Fibre Channel operation on the S5000.

change fc-trace-level

For debugging purposes, change the FC trace level used to record FC information in the trace log.

S5000

Syntax `change fc-trace-level number`

Parameters

number	Trace level used to record FC information in the dump file. Range: 1 to 4, where: • 0 turns FC traces off. • 1 records FC error messages. • 2 records FC warning messages.

- 3 records FC informational messages.
- 4 records all messages generated for FC operation on the switch.

Default: 4.

Defaults	Trace level 4: All FC error messages on the switch are recorded in the FC dump file.
Command Modes	• EXEC • EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Use this command to specify the level of trace information to be included in the FC trace log. To display the trace log, enter the `show file fcmfs:/TRACE_LOG_FC/qstack_trace.log` command.
Example	`FTOS#change fc-trace-level 2`
Related Commands	show fc-trace-level— displays the currently configured FC trace level.

clear counters fibrechannel

Clear Fibre Channel statistics for an FC port.

S5000

Syntax	`clear counters fibrechannel` *`slot/port`*
Parameters	***slot/port*** For *slot*, enter the stack-unit number assigned to the switch. The range of *slot* (stack-unit) numbers is 0 to 11. The range of *port* numbers is 0 to 47.
Defaults	None
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Use the `clear counters fibrechannel` command to clear the statistics (counters) displayed in `show interfaces fibrechannel` command output for a specified FC port.

Example

```
FTOS(conf)#clear counters fibrechannel 0/11
Clear counters on Fc 0/11 [confirm] yes
```

Related Commands	[interface fibrechannel](#) — configures a Fibre Channel interface on the switch. [show interfaces fibrechannel](#) — displays the configuration of a Fibre Channel interface.

create fc-dump-support

Perform a dump of information on S5000 Fibre Channel operation.

S5000

Syntax

```
create fc-dump-support
```

Defaults

None

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use this command to perform a dump of S5000 Fibre Channel operation and store the FC dump file in flash:/CORE_DUMP_DIR. Syslog messages are generated at the start and end of the FC dump file creation.

Example

```
FTOS#create fc-dump-support
```

fabric

Configure the SAN fabric to which a Fibre Channel port connects.

S5000

Syntax

```
fabric fcoe-map
```

Parameters

fcoe-map	Enter the name of the FCoE map which contains the FCoE/FC fabric to which the Fibre Channel port connects.

Defaults

None

Command Modes

INTERFACE FIBRE_CHANNEL

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	Use the `fcoe-map` command to bind an FC port to an FC-FCOE fabric. When a Fibre Channel port operates in N mode, the principal switch in the fabric provides the FCoE Forwarder (FCF) attributes, such as MAC address, FIP priority, and FIP keepalive timeout. To removed the configured FCoE map, enter the `no fabric` command.

Example

```
FTOS(conf)#interface fibrechannel 0/11
FTOS(conf-if-fc-0/11)#fabric SAN_FABRIC_A
```

Related Commands	interface fibrechannel — configures a Fibre Channel interface on the switch. show interfaces fibrechannel — displays the configuration of a Fibre Channel interface.

feature fc

Enable Fibre Channel capability on the S5000.

S5000

Syntax	`feature fc`
Defaults	The S5000 is not enabled to operate in Fibre Channel mode.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Use this command to configure the S5000 to interoperate with Fibre Channel devices in SAN fabrics. Enter the `no feature fc` command to disable the Fibre Channel command-line interface and free memory resources allocated to Fibre Channel operation.

Example

```
FTOS(conf)#feature fc
```

Related Commands	show interfaces fibrechannel — displays the configuration of a Fibre Channel interface.

interface fibrechannel

Configure a Fibre Channel (FC) interface on the switch.

S5000

Syntax	`interface fibrechannel` *`slot/port`*

Parameters

slot/port	For *slot*, enter the stack-unit number assigned to the switch. The range of *slot* (stack-unit) numbers is from 0 to 11. The range of *port* numbers is from 0 to 47. **NOTE:** In release 9.0.(1.3), an FC module can be installed only in expansion slot 0 (ports 0 to 11) on an S5000 switch.

Defaults

By default, a Fibre Channel port is shut down, configured to operate at autosensing speed in N port mode, and to receive Fibre Channel Forwarder (FCF) attributes, such as MAC address, FIP priority, and FC keepalive values, from the principal fabric switch.

By default, the stack-unit number of a standalone S5000 switch is 0.

FC ports are configured by default to operate in N port mode to connect to an F port on an FC switch in a fabric.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can configure a Fibre Channel port to operate at 2G, 4G, or 8G FC speed.

By default, Fibre Channel interfaces are disabled (`shutdown`). When you bring up a Fibre Channel port (`no shutdown`), the Fibre Channel link with a fabric is brought up and the port logs in to a peer switch in the fabric.

When a Fibre Channel port is configured to operate as an NPIV proxy gateway:

- When you shut down the port (`shutdown`), all FCoE virtual links associated with the port are removed.
- When you bring up the port (`no shutdown`), the Fibre Channel link with a fabric is brought up, the FC port logs in to the principal switch, and the fabric starts sending FIP multicast advertisements over downstream 10GbE Ethernet ports. The worldwide name (WWN) received from the principal switch is used as the fabric name in FIP multicast advertisements.

You can apply only one FCoE map on an FC port. When you apply an FCoE map on a fabric-facing FC port, the FC port becomes part of the FCoE fabric, whose settings in the FCoE map are configured on the port and exported to downstream server CNA ports. When you enable a fabric-facing FC port, the FCoE map applied on the port starts sending FIP multicast advertisements using the parameters in the FCoE map over server-facing Ethernet ports. A server sees the FC port with its applied FCoE map as an FCF port.

Example

```
FTOS(conf)#interface fibrechannel 3/0
FTOS(conf-if-fc-3/0)#exit#
```

Related Commands

show interfaces fibrechannel — displays the configuration of a Fibre Channel interface.

show fc-trace-level

Display the currently configured FC trace level.

S5000

Syntax

`show fc-trace-level`

Parameters

None

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `show fc-trace-level` command to display the current trace level used to record FC information in the FC trace file, where:

- 0: FC traces are turned off.
- 1: FC error messages are recorded.
- 2: FC warning messages are recorded.
- 3: FC informational messages are recorded.
- 4: All messages generated for FC operation on the switch are recorded.

To set the FC trace level, use the `change fc-trace-level` command.

Example

```
FTOS#show fc-trace-level
FC Trace Level = 4 (All)
FTOS#
```

Related Commands

change fc-trace-level— changes the FC trace level used to record FC information in the trace log.

show interfaces fibrechannel

Display the configuration of a Fibre Channel interface.

S5000

Syntax

`show interfaces fibrechannel type slot/port`

Parameters

fibrechannel *slot/ port*	Enter the keyword `FibreChannel` followed by slot/port numbers. Valid slot numbers are from 0 to 11. The port range is from 0 to 47.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `show interfaces fibrechannel` command to display the current configuration and operation of a Fibre Channel port on the S5000.

NOTE: In release 9.0.(1.3), an FC module can be installed only in expansion slot 0 (ports 0 to 11) on an S5000 switch.

The following table describes the `show interfaces fibrechannel` command output shown in the following example.

Table 6. Output Fields for the **`show interfaces fibrechannel`** Command

Field	Description
Information:	
Fibrechannel 0/0 is down, FC link is down	Administrative state of. the Fibre Channel interface (up/enabled or down/shutdown) and operational state of the FC link (up or down)
Pluggable media present, SFP+ type	Pluggable optic is. inserted in the port or not, and the SFP+ optic type
Wavelength	Wavelength of the. inserted optic
SFP+ receive power	Power received on SFP. + optic
Interface index	Index number of FC port.
MTU	Maximum transmission. unit on interface (not user-configurable; fixed at 2148 bytes)
LinkSpeed	Configured. Valid link speeds are: transmission speed ofauto (port autosenses the FC port when thespeed of peer FC port), port link is down or2G, 4G, or 8G. current speed when the port link is up

Field	Description
Port type, Max BB credits	The FC port type is fixed. The maximum number at N (end node port)of buffer-to-buffer (BB) credits available is fixed at 16.
WWN, FC-ID	Factory-provided world-. wide name (WWN) of FC port (in hexadecimal) that uniquely identifies the port on the switch (not user-configurable) and the unique FC port ID (24-bit in hexadecimal) received from an FC switch in the fabric after a successful login
Last clearing of "show interface" counters	Elapsed time since the. interface counters displayed in show interfaces output were last cleared
Statistics:	
BBCR_FrameFailures	Number of link resets. due to frames lost during buffer-to-buffer credit recovery (BBCR) period
BBCR_RRDYFrameFailures	Number of link resets. due to multiple Receiver Ready (R_RDY) frames received during the credit recovery period
Class2FramesIn	Number of Class 2. frames received
Class2FramesOut	Number of Class 2. frames transmitted
Class3FramesIn	Number of Class 3. frames received
Class3FramesOut	Number of Class 3. frames transmitted
Class3Discards	Number of Class 3. frames dropped

Field	Description
DecodeErrors	Number of decode. errors
FBusy	Number of Fabric port. Busy (F_BSY) frames received
FReject	Number of Fabric port. Reject (F_RJT) frames received
AddressErrors	Number of frame-. address ID errors
LinkFailures	Number of link failures.
InvalidCRC	Number of cyclic redundancy check (CRC) errors
TotalRxBytes	Number of bytes. received
TotalTxBytes	Number of bytes. transmitted
LongFramesIn	Number of long frames. received
LossOfSync	Number of loss of. synchronization errors
ShortFramesIn	Number of truncated. frames received
RxLinkResets	Number of link resets. on received frames
TxLinkResets	Number of link resets. on transmitted frames
TotalLinkResets	Total number of link. resets
TotalRxFrames	Total number of frames. received
TotalTxFrames	Total number of frames. transmitted
RxOfflineSequences	Number of offline. sequences received
TxOfflineSequences	Number of offline. sequences transmitted
TotalOfflineSequences	Total number of offline. sequences

Field	Description
Rate Information:	
Input bytes/sec, frames/sec, % of line-rate	Incoming rate of FC. traffic in bytes per second, frames per second, and percentage of the total line rate
Output bytes/sec, frames/sec, % of line-rate	Outgoing rate of FC. traffic in bytes per second, frames per second, and percentage of the total line rate
Time since last interface status change	Elapsed time since the. operational status of the interface last changed

Example

```
FTOS#show interfaces fibrechannel 4/0
Fibrechannel 0/0 is down, FC link is down
Pluggable media present, SFP+ type is FC-8GBPS-SR
Wavelength is 850nm
SFP+ receive power reading is -3.4525dBm
Interface index is 33719304
MTU 2148 bytes
LineSpeed auto
Port type is N, Max BB Credits is 16
WWN is 20:00:5c:f9:dd:ef:28:80, FC-ID is 010002
Last clearing of "show interface" counters 05:00:34
Statistics:
    BBCR_FrameFailures 0                     TotalRxBytes
5884
    BBCR_RRDYFailures  0                     TotalTxBytes
18312
    Class2FramesIn     0                     LongFramesIn    0
    Class2FramesOut    0                     LossOfSync      0
    Class3FramesIn     127                   ShortFramesIn   34
    Class3FramesOut    128                   RxLinkResets    0
    Class3Discard      0                     TxLinkResets    1
    DecodeErrors       0                     TotalLinkResets 1
    FReject            0                     TotalRxFrames   127
    FBusy              0                     TotalTxFrames   128
    AddressErrors      0                     RxOfflineSeq    1
    LinkFailures       0                     TxOfflineSeq    3
    InvalidCRC         1                     TotalOfflineSeq 4
Rate info:
    Input 0 bytes/sec, 0 frames/sec, 0.00% of line-rate
    Output 0 bytes/sec, 0 frames/sec, 0.00% of line-rate
    Time since last interface status change: 00:17:56
```

Related Commands

interface fibrechannel — configures a Fibre Channel interface on the switch.

show fc switch

Display the switch configuration for Fibre Channel capability.

S5000

Syntax	`show fc switch`
Parameters	None
Command Modes	• EXEC • EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Usage Information

Use the `show interfaces fibrechannel` command to display information on the Fibre Channel capability of a switch.

The following table describes the `show fc switch` output shown in the following example.

Switch Mode	Fibre Channel mode of operation of an S5000 switch. Default: NPG (configured as an NPIV proxy gateway).
Switch WWN	Factory-assigned worldwide node (WWN) name of the S5000. The S5000 WWN name is not user-configurable.

Example

```
FTOS# show fc switch
Switch Mode : NPG
Switch WWN  : 10:00:5c:f9:dd:ef:10:c0
FTOS#
```

Related Commands

interface fibrechannel — configures a Fibre Channel interface on the switch.

show interfaces fibrechannel — displays the configuration of a Fibre Channel interface.

speed

Set the speed of a Fibre Channel port or configure the port to auto-negotiate its speed with a peer.

S5000

Syntax `speed {auto | 2G | 4G | 8G}`

Parameters

auto	The port autosenses the speed of a peer FC port .
2G	Port speed is 2 gigabits per second (Gbps).
4G	Port speed is 4 Gbps.

8G	Port speed is 8 Gbps.

Defaults An FC port autosenses the speed of a peer FC port.

Command Modes INTERFACE FIBRE_CHANNEL

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information When an FC port autosenses the speed of a peer FC port, it auto-negotiates to determine its speed.

To removed the configured port speed, enter the `no speed {2G | 4G | 8G}` command.

Example

```
FTOS(conf)#interface fibrechannel 0/11
FTOS(conf-if- fc-0/11)#speed 8g
```

Related Commands

interface fibrechannel — configures a Fibre Channel interface on the switch.

show interfaces fibrechannel — displays the configuration of a Fibre Channel interface.

23

IPv4 Routing

The basic IPv4 commands are supported by FTOS on the Dell Networking S5000 switch.

arp

Use address resolution protocol (ARP) to associate an IP address with a MAC address in the switch.

S5000

Syntax

`arp ip-address mac-address interface-type slot/port`

To remove an ARP address, use the `no arp ip-address` command.

Parameters

ip-address	Enter an IP address in dotted decimal format.
mac-address	Enter a MAC address in nnnn.nnnn.nnnn format.
interface-type slot/port	(OPTIONAL) Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You cannot use Class D or Class E IP addresses or zero IP address (0.0.0.0) when creating a static ARP. Zero MAC addresses (00:00:00:00:00:00) are also invalid.

Related Commands	clear arp-cache – clears dynamic ARP entries from the ARP table. show arp – displays the ARP table.

arp learn-enable

Enable ARP learning using gratuitous ARP.

S5000

Syntax	`arp learn-enable`
Defaults	Disabled
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.

arp retries

Set the number of ARP retries in case the system does not receive an ARP reply in response to an ARP request.

S5000

Syntax	`arp retries` *`number`*
Parameters	***number*** Enter the number of retries. The range is 5 to 20. The default is **5**.
Defaults	**5**
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Retries are 20 seconds apart.
Related Commands	show arp retries – displays the configured number of ARP retries.

arp timeout

Set the time interval for an ARP entry to remain in the ARP cache.

S5000

Syntax

```
arp timeout minutes
```

Parameters

seconds	Enter the number of minutes. The range is 0 to 35790. The default is **240 minutes**.

Defaults **240 minutes** (4 hours)

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands show interfaces – displays the ARP timeout value for all available interfaces.

clear arp-cache

Clear the dynamic ARP entries from a specific interface or optionally delete (`no-refresh`) ARP entries from the content addressable memory (CAM).

S5000

Syntax

```
clear arp-cache [interface-type slot/port | ip ip-address] [no-
refresh]
```

Parameters

interface-type slot/port	(OPTIONAL) Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

ip *ip-address*	(OPTIONAL) Enter the keyword `ip` followed by the IP address of the ARP entry you wish to clear.
no-refresh	(OPTIONAL) Enter the keywords `no-refresh` to delete the ARP entry from CAM. Or use this option with *`interface`* or `ip` *`ip-address`* to specify which dynamic ARP entries you want to delete. **NOTE:** Transit traffic may not be forwarded during the period when deleted ARP entries are resolved again and re-installed in CAM. Use this option with extreme caution.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear host

Remove one or all dynamically learned host table entries.

S5000

Syntax

```
clear host name
```

Parameters

name	Enter the name of the host to delete. Enter `*` to delete all host table entries.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ip fib stack-unit

Clear all forwarding information base (fib) entries in the specified stack-unit (use this command with caution, refer to *Usage Information* below).

S5000

Syntax

```
clear ip fib stack—unit unit-number
```

Parameters

stack-unit *unit-number*	Enter the keyword `stack-unit` followed by the unit number. The range is 0 to 11.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use this command to clear Layer 3 CAM inconsistencies.

△ **CAUTION: Executing this command causes traffic disruption.**

Related Commands

show ip fib stack-unit – shows FIB entries.

clear ip route

Clear one or all routes in the routing table.

S5000

Syntax

```
clear ip route {* | ip-address mask }
```

Parameters

*	Enter an asterisk (*) to clear all learned IP routes.
ip-address mask	Enter a specific IP address and mask in dotted decimal format to clear that IP address from the routing table.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

ip route – assigns an IP route to the switch.

show ip route – views the routing table.

show ip route summary – views a summary of the routing table.

clear tcp statistics

Clear TCP counters.

S5000

Syntax

```
clear tcp statistics
```

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug arp

View information on ARP transactions.

S5000

Syntax

`debug arp [`*`interface-type slot/port`*`] [count`*`value`*`]`

To stop debugging ARP transactions, use the `no debug arp` command.

Parameters

interface-type slot/port	(OPTIONAL) Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
count ***value***	(OPTIONAL) Enter the keyword `count` followed by the count value. The range is 1 to 65534.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `count` option to stop packets from flooding the user terminal when debugging is turned on.

debug ip dhcp

Enable debug information for dynamic host configuration protocol (DHCP) relay transactions and display the information on the console.

S5000

Syntax	`debug ip dhcp` To disable debug, use the `no debug ip dhcp` command.
Defaults	Debug disabled
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
FTOS#debug ip dhcp
00:12:21 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received
at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xbf05140f, secs = 0, hwaddr =
00:60:CF:20:7B:8C, teaddr = 0.0.0.0
00:12:21 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for
00:60:CF:20:7B:8C to 14.4.4.2
00:12:26 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received
at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xbf05140f, secs = 5, hwaddr =
00:60:CF:20:7B:8C, teaddr = 0.0.0.0
00:12:26 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for
00:60:CF:20:7B:8C to 14.4.4.2
00:12:40 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received
at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr =
00:60:CF:20:7B:8C, teaddr = 0.0.0.0
00:12:40 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for
00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at
interface 14.4.4.1 BOOTP Reply,
hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:
8C, teaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for
00:60:CF:20:7B:8C to 113.3.3.254
00:12:42 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received
at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr =
00:60:CF:20:7B:8C, teaddr = 0.0.0.0
00:12:42 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for
00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at
interface 14.4.4.1 BOOTP Reply,
hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:
8C, teaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for
00:60:CF:20:7B:8C to 113.3.3.254
FTOS#
```

Related Commands	ip helper-address – specifies the destination broadcast or host address for the DHCP server request.

ip helper-address hop-count disable – disables the hop-count increment for the DHCP relay agent.

debug ip icmp

View information on the internal control message protocol (ICMP).

S5000

Syntax

`debug ip icmp [interface-type slot/port] [count value]`

To disable debugging, use the `no debug ip icmp` command.

Parameters

interface-type slot/port	(OPTIONAL) Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
count *value*	(OPTIONAL) Enter the keyword `count` followed by the count value. The range is 1 to 65534. The default is **Infinity**.

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
ICMP: echo request rcvd from src 40.40.40.40
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: echo request sent to dst 40.40.40.40
ICMP: echo request rcvd from src 40.40.40.40
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: echo request sent to dst 40.40.40.40
```

Usage Information	Use the `count` option to stop packets from flooding the user terminal when debugging is turned on.

debug ip packet

View a log of IP packets sent and received.

S5000

Syntax

`debug ip packet [access-group name] [count value] [interface-type slot/port]`

To disable debugging, use the `no debug ip packet [access-group name] [count value] [interface-type slot/port]` command.

Parameters

access-group *name*	Enter the keyword `access-group` followed by the access list name (maximum 16 characters) to limit the debug output based on the defined rules in the ACL.
count *value*	(OPTIONAL) Enter the keyword `count` followed by the count value. The range is 1 to 65534. The default is `Infinity`.
interface-type slot/port	(OPTIONAL) Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `debug ip packet` command in the Example below.

Field	**Description**

s=	Lists the source address of the packet and the name of the interface (in parentheses) that received the packet.
d=	Lists the destination address of the packet and the name of the interface (in parentheses) through which the packet is being sent out on the network.
len	Displays the packet's length.
sending, rcvd, fragment, sending broad/ multicast proto, unroutable	The last part of each line lists the status of the packet.
TCP src=	Displays the source and destination ports, the sequence number, the acknowledgement number, and the window size of the packets in that TCP packets.
UDP src=	Displays the source and destination ports for the UDP packets.
ICMP type=	Displays the ICMP type and code.
IP Fragment	States that it is a fragment and displays the unique number identifying the fragment (Ident) and the offset (in 8-byte units) of this fragment (fragment offset) from the beginning of the original datagram.

Example

```
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 54, sending
    TCP src=23, dst=40869, seq=2112994894, ack=606901739,
win=8191 ACK PUSH
IP: s=10.1.2.206 (Ma 0/0), d=10.1.2.62, len 40, rcvd
    TCP src=0, dst=0, seq=0, ack=0, win=0
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 226,
sending
    TCP src=23, dst=40869, seq=2112994896, ack=606901739,
win=8192 ACK PUSH
IP: s=10.1.2.216 (Ma 0/0), d=10.1.2.255, len 78, rcvd
    UDP src=0, dst=0
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500,
sending fragment
    IP Fragment, Ident = 4741, fragment offset = 0
    ICMP type=0, code=0
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500,
sending fragment
    IP Fragment, Ident = 4741, fragment offset = 1480
IP: s=40.40.40.40 (local), d=224.0.0.5 (Te 4/11), len 64,
sending broad/multicast
proto=89
IP: s=40.40.40.40 (local), d=224.0.0.6 (Te 4/11), len 28,
sending broad/multicast
proto=2
IP: s=0.0.0.0, d=30.30.30.30, len 100, unroutable
   ICMP type=8, code=0
IP: s=0.0.0.0, d=30.30.30.30, len 100, unroutable
   ICMP type=8, code=0
```

Usage Information

Use the `count` option to stop packets from flooding the user terminal when debugging is turned on.

The `access-group` option supports only the equal to (`eq`) operator in TCP ACL rules. Port operators not equal to (`neq`), greater than (`gt`), less than (`lt`), or `range` are not supported in access-group option (refer to the Example below). ARP packets (`arp`) and Ether-type (`ether-type`) are also not supported in the `access-group` option. The entire rule is skipped to compose the filter.

The `access-group` option pertains to:

- IP Protocol Number: 0 to 255
- Internet Control Message Protocol (`icmp`) but not the ICMP message type (0-255)
- Any Internet Protocol (`ip`)
- Transmission Control Protocol (`tcp`) but not on the `rst`, `syn`, or `urg` bits
- User Datagram Protocol (`udp`)

In the case of ambiguous access control list rules, the `debug ip packet access-control` command is disabled. A message appears identifying the error (refer to the Example below).

Example (Error Messages)

```
FTOS#debug ip packet access-group test
%Error: port operator GT not supported in access-list debug
%Error: port operator LT not supported in access-list debug
%Error: port operator RANGE not supported in access-list debug
%Error: port operator NEQ not supported in access-list debug

FTOS#00:10:45: %STKUNIT0-M:CP
%IPMGR-3-DEBUG_IP_PACKET_ACL_AMBIGUOUS_EXP: Ambiguous rules not
supported in access-list debug, access-list debugging is
turned off
FTOS#
```

ip address

Assign a primary and secondary IP address to the interface.

S5000

Syntax

`ip address` *`ip-address mask`* `[secondary]`

To delete an IP address from an interface, use the `no ip address [`*`ip-address`*`]` command.

Parameters

ip-address	Enter an IP address in dotted decimal format.
mask	Enter the mask of the IP address in slash prefix format (for example, /24).
secondary	(OPTIONAL) Enter the keyword `secondary` to designate the IP address as the secondary address.

Defaults

Not configured.

Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	You must be in INTERFACE mode before you add an IP address to an interface. Assign an IP address to an interface prior to entering ROUTER OSPF mode.

ip directed-broadcast

Enables the interface to receive directed broadcast packets.

S5000

Syntax	`ip directed-broadcast` To disable the interface from receiving directed broadcast packets, use the `no ip directed-broadcast` command.
Defaults	Disabled (that is, the interface does not receive directed broadcast packets)
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ip domain-list

Configure names to complete unqualified host names.

S5000

Syntax	`ip domain-list` *`name`* To remove the name, use the `no ip domain-list` *`name`* command.
Parameters	***name*** Enter a domain name to be used to complete unqualified names (that is, incomplete domain names that cannot be resolved).
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Configure the `ip domain-list` command up to six times to configure a list of possible domain names. If you configure both the `ip domain-name` and `ip domain-list` commands, the software tries to resolve the name using the `ip domain-name` command. If the name is not

resolved, the software goes through the list of names configured with the `ip domain-list` command to find a match.

Use the following steps to enable dynamic resolution of hosts:

- specify a domain name server with the `ip name-server` command
- enable DNS with the `ip domain-lookup` command

To view current bindings, use the `show hosts` command. To view DNS related configuration, use the `show running-config resolve` command.

Related Commands

ip domain-name – specifies a DNS server.

ip domain-lookup

Enable dynamic host-name to address resolution (that is, DNS).

S5000

Syntax

```
p domain-lookup
```

To disable DNS lookup, use the `no ip domain-lookup` command.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To fully enable DNS, also specify one or more domain name servers with the `ip name-server` command.

FTOS does not support sending DNS queries over a VLAN. DNS queries are sent out all other interfaces, including the Management port.

To view current bindings, use the `show hosts` command.

Related Commands

ip name-server – specifies a DNS server.

show hosts – Views the current bindings.

ip domain-name

Configure one domain name for the switch.

S5000

Syntax

`ip domain-name name`

To remove the domain name, use the `no ip domain-name` command.

Parameters

name	Enter one domain name to be used to complete unqualified names (that is, incomplete domain names that cannot be resolved).

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can only configure one domain name with the `ip domain-name` command. To configure more than one domain name, configure the `ip domain-list` command up to six times.

Use the following steps to enable dynamic resolution of hosts:

- specify a domain name server with the `ip name-server` command
- enable DNS with the `ip domain-lookup` command

To view current bindings, use the `show hosts` command.

Related Commands

ip domain-list – configures additional names.

ip helper-address

Specify the address of a DHCP server so that DHCP broadcast messages can be forwarded when the DHCP server is not on the same subnet as the client.

S5000

Syntax

`ip helper-address ip-address`

To remove a DHCP server address, use the `no ip helper-address` command.

Parameters

ip-address	Enter an IP address in dotted decimal format (A.B.C.D).

Defaults Not configured.

Command Modes INTERFACE

Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	You can add multiple DHCP servers by entering the `ip helper-address` command multiple times. If multiple servers are defined, an incoming request is sent simultaneously to all configured servers and the reply is forwarded to the DHCP client. FTOS uses standard DHCP ports, that is UDP ports 67 (server) and 68 (client) for DHCP relay services. It listens on port 67 and if it receives a broadcast, the software converts it to unicast, and forwards to it to the DHCP-server with source port=68 and destination port=67. The server replies with source port=67, destination port=67 and FTOS forwards to the client with source port=67, destination port=68.

ip helper-address hop-count disable

Disable the hop-count increment for the DHCP relay agent.

S5000

Syntax	`ip helper-address hop-count disable` To re-enable the hop-count increment, use the `no ip helper-address hop-count disable` command.
Defaults	Enabled; the hops field in the DHCP message header is incremented by default.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	This command disables the incrementing of the hops field when boot requests are relayed to a DHCP server through FTOS. If the incoming boot request already has a non-zero hops field, the message is relayed with the same value for hops. However, the message is discarded if the hops field exceeds 16, to comply with the relay agent behavior specified in RFC 1542.
Related Commands	ip helper-address – specifies the destination broadcast or host address for DHCP server requests. show running-config – displays the current configuration and changes from the default values.

ip host

Assign a name and IP address to be used by the host-to-IP address mapping table.

S5000

Syntax

`ip host name ip-address`

To remove an IP host, use the `no ip host name [ip-address]` command.

Parameters

name	Enter a text string to associate with one IP address.
ip address	Enter an IP address, in dotted decimal format, to be mapped to the name.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip max-frag-count

Set the maximum number of fragments allowed in one packet for packet re-assembly.

S5000

Syntax

`ip max-frag-count count`

To place no limit on the number of fragments allowed, use the `no ip max-frag-count` command.

Parameters

count	Enter a number for the number of fragments allowed for re-assembly. The range is 2 to 256.

Defaults No limit is set on number of fragments allowed.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information To avoid denial of service (DOS) attacks, keep the number of fragments allowed for re-assembly low.

ip mtu

Set the IP MTU (frame size) of the packet transmitted by the stack-unit. If the packet must be fragmented, FTOS sets the size of the fragmented packets to the size specified in this command.

S5000

Syntax

`ip mtu value`

To return to the default IP MTU value, use the `no ip mtu` command.

Parameters

value	Enter the maximum MTU size if the IP packet is fragmented. The range is 576 to 9234. The default is **1500 bytes**.

Defaults

1500 bytes

Command Modes

INTERFACE (Gigabit Ethernet and 10 Gigabit Ethernet interfaces)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you enter the `no mtu` command, FTOS reduces the ip mtu value to 1536 bytes. To return the IP MTU value to the default, use the `no ip mtu` command.

You must compensate for Layer 2 header when configuring link MTU on an Ethernet interface or FTOS may not fragment packets. If the packet includes a Layer 2 header, the difference between the link MTU and IP MTU (the `ip mtu` command) must be enough bytes to include for the Layer 2 header.

Link MTU and IP MTU considerations for Port Channels and VLANs are as follows

Port Channels:

- All members must have the same link MTU value and the same IP MTU value.
- The Port Channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members. For example, if the members have a link MTU of 2100 and an IP MTU 2000, the Port Channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

VLANs:

- All members of a VLAN must have same IP MTU value.
- Members can have different Link MTU values. Tagged members must have a link MTU 4 bytes higher than untagged members to account for the packet tag.
- The VLAN link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the VLAN members. For example, the VLAN contains tagged members with Link MTU of 1522 and IP MTU of 1500 and untagged members with Link MTU of 1518 and IP MTU of 1500. The VLAN's Link MTU cannot be higher than 1518 bytes and its IP MTU cannot be higher than 1500 bytes.

The following describes the difference between Link MTU and IP MTU for Layer 2 overhead.

Ethernet (untagged)	18 bytes
VLAN Tag	Tag 22 bytes

Untagged Packet with VLAN-Stack Header	22 bytes
Tagged Packet with VLAN-Stack Header	26 bytes

Related Commands

mtu – sets the link MTU for an Ethernet interface.

ip name-server

Enter up to six IPv4 addresses of name servers. The order you enter the addresses determines the order of their use.

S5000

Syntax

`ip name-server ipv4-address [ipv4-address2...ipv4-address6]`

To remove a name server, use the `no ip name-server ip-address` command.

Parameters

ipv4-address	Enter the IPv4 address, in dotted decimal format, of the name server to be used.
ipv4-address2... ipv4-address6	(OPTIONAL) Enter up five more IPv4 addresses, in dotted decimal format, of name servers to be used. Separate the addresses with a space.

Defaults

No name servers are configured.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

FTOS does not support sending DNS queries over a VLAN. DNS queries are sent out on all other interfaces, including the Management port.

You can separately configure both IPv4 and IPv6 domain name servers.

Related Commands

ipv6 name-server – configures an IPv6 name server.

ip proxy-arp

Enable proxy ARP on an interface.

S5000

Syntax	`ip proxy-arp` To disable proxy ARP, use the `no ip proxy-arp` command.
Defaults	Enabled.
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	show ip interface – displays the interface routing status and configuration.

ip route

Assign a static route to the switch.

S5000

Syntax

`ip route {[ destination | mask | ip-address | interface-type slot/port | distance ]} [permanent] [tag tag-value]`

To delete a specific static route, use the `no ip route destination mask {address | interface-type slot/port [ip-address]}` command.

To delete all routes matching a certain route, use the `no ip route destination mask` command.

Parameters

destination	Enter the IP address in dotted decimal format of the destination device.
mask	Enter the mask in slash prefix formation (/x) of the destination device's IP address.
ip-address	Enter the IP address in dotted decimal format of the forwarding router.
interface-type slot/port	Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

- For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
- For a Null interface, enter the keywords `null 0`.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

distance	(OPTIONAL) Enter a number as the distance metric assigned to the route. The range is 1 to 255.
permanent	(OPTIONAL) Enter the keyword `permanent` to specify the route is not removed, even if the interface assigned to that route goes down. The route must be up initially to install it in the routing table.
tag ***tag-value***	(OPTIONAL) Enter the keyword `tag` followed by a number to assign to the route. The range is 1 to 4294967295.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Using the following example of a static route: ip route 33.33.33.0 /24 tengigabitethernet 0/0 172.31.5.43

- The software installs a next hop that is not on the directly connected subnet but which recursively resolves to a next hop on the interface's configured subnet. In the example, if tengigabitethernet 0/0 has an ip address on subnet 2.2.2.0 and if 172.31.5.43 recursively resolves to 2.2.2.0, FTOS installs the static route.
- When the interface goes down, FTOS withdraws the route.
- When the interface comes up, FTOS re-installs the route.
- When recursive resolution is "broken," FTOS withdraws the route.
- When recursive resolution is satisfied, FTOS re-installs the route.

Related Commands show ip route – views the switch routing table.

ip source-route

Enable FTOS to forward IP packets with source route information in the header.

S5000

Syntax `ip source-route`

To drop packets with source route information, use the `no ip route-source` command.

Defaults	Enabled.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ip unreachables

Enable the generation of internet control message protocol (ICMP) unreachable messages.

S5000

Syntax	`ip unreachables` To disable the generation of ICMP messages, use the `no ip unreachables` command.
Defaults	Disabled.
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

load balance

By default, for the S5000, FTOS uses an IP 4-tuple (IP SA, IP DA, Source Port, and Destination Port) to distribute IP traffic over members of a Port Channel as well as equal-cost paths. To designate another method to balance traffic over Port Channel members, use the `load-balance` command.

S5000

Syntax

```
load-balance {ip-selection [dest-ip | source-ip]} | {mac [dest-
mac | source-dest-mac | source-mac]} | {tcp-udp | ingress-port
[enable]}
```

To return to the default setting (IP 4-tuple), use the `no load-balance {ip-selection [dest-ip | source-ip]} | {mac [dest-mac | source-dest-mac | source-mac]} | {tcp-udp | ingress-port [enable]}` command.

Parameters

ip-selection {dest-ip | source-ip}	Enter the keywords to distribute IP traffic based on the following criteria: • `dest-ip` — Uses destination IP address and destination port fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded. • `source-ip` — Uses source IP address and source port fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded.

mac {dest-mac | source-dest-mac | source-mac}	Enter the keywords to distribute MAC traffic based on the following criteria: • `dest-mac` — Uses the destination MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded. • `source-dest-mac` — Uses the destination and source MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded. • `source-mac` — Uses the source MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded.
tcp-udp enable	Enter the keywords to distribute traffic based on the following: • `enable` — Takes the TCP/UDP source and destination ports into consideration when doing hash computations. (By default, this is **enabled**.)
ingress-port enable	Enter the keywords to distribute traffic based on the following: • `enable` — Takes the source port into consideration when doing hash computations. (By default, this is **disabled**.)

Defaults IP 4-tuple (IP SA, IP DA, Source Port, Destination Port)

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information By default, FTOS distributes incoming traffic based on a hash algorithm using the following criteria:

- IP source address
- IP destination address
- TCP/UDP source port
- TCP/UDP destination port

Related Commands hash-algorithm ecmp – changes the hash algorithm across an ECMP.

management route

Configure a static route that points to the Management interface or a forwarding router.

S5000

Syntax

```
management route {ipv4-address | ipv6-address}/mask
{forwarding-router-address | managementethernet}
```

Parameters

{ipv4-address | ipv6-address}/ mask	Enter an IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X), followed by the prefix-length for the IP address of the management interface. **NOTE:** The :: notation in an IPv6 address specifies successive hexadecimal fields of zero. Only one occurrence of this notation is permitted in an IPv6 address.
forwarding-router-address	Enter an IPv4 or IPv6 address of a forwarding router.
managementethernet	Enter the keyword `managementethernet` for the Management interface on the Primary Stack-unit.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When a static route (or a protocol route) overlaps with Management static route, the static route (or a protocol route) is preferred over the Management Static route. Also, Management static routes and the Management Connected prefix are not reflected in the hardware routing tables. Separate routing tables are maintained for IPv4 and IPv6 management routes. This command manages both tables.

Related Commands

interface ManagementEthernet – configures the Management port on the system (either the primary or standby stack-unit).

duplex (Management) – sets the mode of the Management interface.

speed (Management interface) – sets the speed for the Management interface.

show arp

Display the ARP table.

S5000

Syntax

```
show arp [inspection | interface type slot/port | ip ip-address
[mask] | macaddress mac-address [mac-address mask] | retries]
[static | dynamic] [summary]
```

Parameters

inspection	(OPTIONAL) Enter the keyword `inspection` followed by `database` or `statistics` to view dynamic ARP inspection details.
interface *type slot/port*	(OPTIONAL) Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
ip *ip-address mask*	(OPTIONAL) Enter the keyword `ip` followed by an IP address in the dotted decimal format. Enter the optional IP address mask in the slash prefix format (/ x).
macaddress *mac-address mask*	(OPTIONAL) Enter the keyword `macaddress` followed by a MAC address in nn:nn:nn:nn:nn:nn format. Enter the optional MAC address mask in nn:nn:nn:nn:nn format also.
retries	(OPTIONAL) Enter the keyword `retries` to view the number of ARP retries before a 20 sec back off.
static	(OPTIONAL) Enter the keyword `static` to view entries entered manually.
dynamic	(OPTIONAL) Enter the keyword `dynamic` to view dynamic entries.
summary	(OPTIONAL) Enter the keyword `summary` to view a summary of ARP entries.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The Example below shows two VLANs that are associated with a private VLAN (PVLAN) (refer to Private VLAN (PVLAN)).

The following describes the `show arp` command shown in the Example below.

Row Heading	Description
Protocol	Displays the protocol type.

Address	Displays the IP address of the ARP entry.
Age(min)	Displays the age (in minutes) of the ARP entry.
Hardware Address	Displays the MAC address associated with the ARP entry.
Interface	Displays the first two letters of the interfaces type and the slot/port associated with the ARP entry.
VLAN	Displays the VLAN ID, if any, associated with the ARP entry.
CPU	Lists which CPU the entries are stored on.

Example

```
FTOS#show arp

Protocol Address  Age  Hardware Address  Interface VLAN CPU
                 (min)
-----------------------------------------------------------
Internet 10.11.1.1  80 00:01:e9:45:00:03 Ma 0/0     -   CP
Internet 10.11.8.5 207 00:01:e9:45:00:03 Ma 0/0     -   CP
Internet 10.11.8.5 233 00:01:e9:45:00:03 Ma 0/0     -   CP
Internet 10.11.9.1 206 00:01:e9:45:00:03 Ma 0/0     -   CP
Internet 10.11.51.1 85 00:01:e9:45:00:03 Ma 0/0     -   CP
FTOS#
```

Example (Private VLAN)

NOTE: In this example, Line 1 shows community VLAN 200 (in primary VLAN 10) in a PVLAN. Line 2 shows primary VLAN 10.

```
FTOS#show arp

Protocol Address  Age Hardware Address Interface  VLAN      CPU
                 (min)
---------------------------------------------------------------
Internet 5.5.5.1   -  00:01:e8:43:96:5e -         Vl 10 pv20 CP
Internet 5.5.5.10  -  00:01:e8:44:99:55 -         Vl 10      CP
Internet 10.1.2.4  1  00:01:e8:d5:9e:e2 Ma 0/0    -          CP
Internet 10.1.1.3  1  00:01:e8:d5:9e:e2 Ma 0/0    -          CP
Internet 10.1.1.4  1  00:01:e8:d5:9e:e2 Ma 0/0    -          CP
Internet 10.1.1.5  2  00:01:e8:d5:9e:e2 Ma 0/0    -          CP
Internet 13.3.3.4  1  00:01:e8:d5:9e:e2 Ma 0/0    -          CP
```

Usage Information

The following describes the `show arp summary` command shown in the Example below.

Row Heading	Description
Total Entries	Lists the total number of ARP entries in the ARP table.
Static Entries	Lists the total number of configured or static ARP entries.
Dynamic Entries	Lists the total number of learned or dynamic ARP entries.
CPU	Lists the CPU entries are stored on.

Example (Summary)

```
#show arp summary

TotalEntries   Static Entries   Dynamic Entries   CPU
----------------------------------------------------
83             0                83                CP
FTOS
```

Related Commands	ip local-proxy-arp – enables/disables Layer 3 communication in secondary VLANs. switchport mode private-vlan – sets PVLAN mode of the selected port.

show arp retries

Display the configured number of ARP retries.

S5000

Syntax

```
show arp retries
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

arp retries – sets the number of ARP retries in case the system does not receive an ARP reply in response to an ARP request.

show hosts

View the host table and DNS configuration.

S5000

Syntax

```
show hosts
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show hosts` command in the Example below.

Field	**Description**
Default domain...	Displays the domain name (if configured).
Name/address lookup...	States if DNS is enabled on the system. • If DNS is enabled, the Name/Address lookup is domain service.

	- If DNS is not enabled, the Name/Address lookup is static mapping
Name servers are...	Lists the name servers, if configured.
Host	Displays the host name assigned to the IP address.
Flags	Classifies the entry as one of the following: - perm - the entry was manually configured and will not time out - temp - the entry was learned and will time out after 72 hours of inactivity. Also included in the flag is an indication of the validity of the route: - ok - the entry is valid. - ex - the entry expired. - ?? - the entry is suspect.
TTL	Displays the amount of time until the entry ages out of the cache. For dynamically learnt entries only.
Type	Displays IP as the type of entry.
Address	Displays the IP address(es) assigned to the host.

Example

```
FTOS#show hosts
Default domain is not set
Name/address lookup uses static mappings
Name servers are not set
Host     Flags      TTL   Type   Address
-------- -----      ----  ----   -------
ks       (perm, OK) -     IP     2.2.2.2
4200-1   (perm, OK) -     IP     192.68.69.2
1230-3   (perm, OK) -     IP     192.68.99.2
ZZr      (perm, OK) -     IP     192.71.18.2
Z10-3    (perm, OK) -     IP     192.71.23.1
FTOS#
```

Related Commands

traceroute – views the DNS resolution.

ip host – configures a host.

show ip cam stack-unit

Display CAM entries for the S5000 switch.

S5000

Syntax

```
show ip cam stack-unit unit-number port-set pipe-number [ip-
address mask [longer-prefixes] | ecmp-group | member-info |
detail | summary]
```

Parameters

stack-unit ***unit-number***	Enter the keyword `stack-unit` followed by the unit number. The range is 0 to 11.
port-set ***pipe-number***	Enter the keyword `port-set` followed by number of the port-pipe. Values are 0 or 1.
ip-address mask **[longer-prefix]**	(OPTIONAL) Enter the IP address and mask of a route to CAM entries for that route only. Enter the keyword `longer-prefixes` to view routes with a common prefix.
detail	Enter the keyword `detail` to display the group index ID used by the ecmp routes in the CAM.
member-info	Enter the keyword `member-info` to display the group index used by the ecmp, the number of egress ports (members) for the ecmp, and the port details of each member. The detail information under member-info gives the MAC address, VLAN ID, and gateway of every member port of the ecmp.
summary	(OPTIONAL) Enter the keyword `summary` to view a table listing route prefixes and the total number routes which can be entered in to CAM.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip cam` command shown in the Example below.

Field	**Description**
Destination	Displays the destination route of the index.
CG	Displays 0.
V	Displays a 1 if the entry is valid and a 0 otherwise.
C	Displays the CPU bit. 1 indicates that a packet hitting this entry is forwarded to the CP depending on egress port.
V Id	Displays the VLAN ID. If the entry is 0, the entry is not part of a VLAN.
Mac Addr	Displays the next-hop router’s MAC address.

Port	Displays the egress interface. Use the second half of the entry to determine the interface. For example, in the entry 17cl CP, the CP is the pertinent portion. • CP = control processor • Gi = Gigabit Ethernet interface • Te = 10 Gigabit Ethernet interface

Example

```
FTOS#show ip cam stack-unit 0 port-set 0 10.10.10.10/32 longer-
prefixes

Destination   EC CG V C VId    Mac-Addr            Port
----------------- -- -- - ------ --------------------
10.10.10.10   0 0 1 1 0    00:00:00:00:00:00   3f01 CP
FTOS#
```

Usage Information

The following describes the `show ip cam ecmp-group` command shown in the Example below.

Field	Description
Prefix Length	Displays the prefix-length or mask for the IP address configured on the stack-unit 0 port pipe 0.
Current Use	Displays the number of routes currently configured for the corresponding prefix or mask on the stack-unit 0 port pipe 0.
Initial Size	Displays the CAM size allocated by FTOS for the corresponding mask. The CAM size is adjusted by FTOS if the number of routes for the mask exceeds the initial allocation.

Example (ecmp-group)

```
FTOS#show ip cam stack-unit 0 po 0 ecmp-group detail

Destination EC CG V C VId Mac-Addr        Port ECMP Group-Index
----------------- -- -- - ----- ---------------- -------------
1.1.1.2       0 0 1 0   0 00:01:e8:8a:d6:58    0004 Te 0/3    -
2.1.1.2       0 0 1 0   0 00:01:e8:8a:d6:58    0009 Te 0/8    -
1.1.1.1       0 0 1 1   0 00:00:00:00:00:00    3f01 CP        -
2.1.1.1       0 0 1 1   0 00:00:00:00:00:00    3f01 CP        -
1.1.1.0       0 0 1 1   0 00:00:00:00:00:00    3f01 CP        -
2.1.1.0       0 0 1 1   0 00:00:00:00:00:00    3f01 CP        -
100.1.1.      0 1 0 1   0 0 00:01:e8:8a:d6:58  0004 Te 0/3    0
100.1.1.      0 1 0 1   0 0 00:01:e8:8a:d6:58  0009 Te 0/8    0
0.0.0.0       0 0 1 1   0 00:00:00:00:00:00    3f01 CP        -
FTOS#
```

Example (Member-Info)

```
FTOS#show ip cam stack-unit 0 po 0 ecmp-group member-info
detail

Group Index Member Count  Mac-Addr       Port   VLan ID  Gateway
----------- --------------------------------- ------------------
  0         2       00:01:e8:8a:d6:58   Te 0/3   0    1.1.1.2
                    00:01:e8:8a:d6:58   Te 0/8   0    2.1.1.2
FTOS#
```

show ip fib stack-unit

View all FIB entries.

S5000

Syntax

```
show ip fib stack-unit unit-number [ip-address [mask] [longer-prefixes] | summary]
```

Parameters

stack-unit *unit-number*	Enter the keyword `stack-unit` followed by the unit number. The range is 0 to 11.
ip-address mask	(OPTIONAL) Enter the IP address of the network destination to view only information on that destination. Enter the IP address in dotted decimal format (A.B.C.D). You must enter the mask in slash prefix format (/X).
longer-prefixes	(OPTIONAL) Enter the keywords `longer-prefixes` to view all routes with a common prefix.
summary	(OPTIONAL) Enter the keyword `summary` to view the total number of prefixes in the FIB.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip fib stack-unit` command shown in the Example below.

Field	**Description**
Destination	Lists the destination IP address.
Gateway	Displays either the word “direct” and an interface for a directly connected route or the remote IP address to be used to forward the traffic.
First-Hop	Displays the first hop IP address.
Mac-Addr	Displays the MAC address.
Port	Displays the egress-port information.
Vld	Displays the VLAN ID. If no VLAN is assigned, zero (0) is listed.
EC	Displays the number of ECMP paths.

Example

```
FTOS#show ip fib stack-unit 0

Destination     Gateway       First-Hop    Mac-Addr
------------------------------------------------------
10.10.10.10/32 Direct, Nu 0  0.0.0.0    00:00:00:00:00:00
```

```
Port    VId EC
-------------
BLK HOLE 0 0
FTOS>
```

Related Commands	clear ip fib stack-unit – clears the FIB entries on a specified stack-unit.

show ip flow

Show how a Layer 3 packet is forwarded when it arrives at a particular interface.

S5000

Syntax

`show ip flow interface [type slot/port {source-ip-address destination-ip-address } {protocol [tcp | udp | number ]} {source-port port-number destination-port port-number}`

Parameters

interface *type slot/port*	Enter the keyword *interface* followed by of the following interface keywords. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
source-ip-address	Enter the source IP address.
destination-ip-address	Enter the destination IP address.
source-port *port-number*	Enter the keywords *source-port* followed by the source port number.
destination-port *port-number*	Enter the keywords *destination-port* followed by the destination port number.

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command provides egress port information for a given IP flow. This is useful in identifying which interface the packet follows in the case of Port-channel and Equal Cost Multi Paths. Use this command for routed packets only. For switched packets, use the `show port-channel-flow` command.

The `show ip flow` command does not compute the egress port information when `load-balance mac hashing` is also configured due to insufficient information (the egress MAC is not available).

The S5000 produces the following error message: `%Error: Unable to read IP route table.`

Example

```
FTOS#show ip flow interface Te 1/8 189.1.1.1 63.0.0.1 protocol
tcp source-port 7898 destination-port 8
```

flow: 189.1.1.1 63.0.0.1 protocol 6 7868 8976

```
Ingress interface:Te 1/20
Egress interface:Te 1/14 to 1.7.1.2[CAM hit 103710]
unfragmented packet
                 Te 1/10 to 1.2.1.2[CAM hit 103710] fragmented
packet
```

show ip interface

View IP-related information on all interfaces.

S5000

Syntax

`show ip interface [`*`type slot/port`*` | brief | stack—unit `*`unit-number`*`] [configured]`

Parameters

interface *type slot/port*	(OPTIONAL) Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0. • For a Null interface, enter the keywords `null 0`. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094. • For a stack-unit, enter the keyword `stack-unit` followed by the stack-unit number. The range is 0 to 11.

brief	(OPTIONAL) Enter the keyword `brief` to view a brief summary of the interfaces and whether an IP address is assigned.
configured	(OPTIONAL) Enter the keyword `configured` to display the physical interfaces with non-default configurations only.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output for the `show ip interface` command shown in the Example below.

Field	Description
TenGigabitEthernet 0/0...	Displays the interface's type, slot/port, and physical and line protocol status.
Internet address...	States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.
IP MTU is...	Displays IP MTU value.
Inbound access...	Displays the name of the any configured incoming access list. If none is configured, the phrase "not set" is displayed.
Proxy ARP...	States whether proxy ARP is enabled on the interface.
Split horizon...	States whether split horizon for RIP is enabled on the interface.
Poison Reverse...	States whether poison for RIP is enabled on the interface.
ICMP redirects...	States if ICMP redirects are sent.
ICMP unreachables...	States if ICMP unreachable messages are sent.

Example

```
FTOS#show ip int te 0/0
TenGigabitEthernet 0/0 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Inbound access list is not set
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent

FTOS#
```

Usage Information

The following describes output for the `show ip interface brief` command shown in the Example below.

Column Heading	Description

Interface	Displays type of interface and the associated slot and port number.
IP-Address	Displays the IP address for the interface, if configured.
Ok?	Indicates if the hardware is functioning properly.
Method	Displays “Manual” if the configuration is read from the saved configuration.
Status	States whether the interface is enabled (up) or disabled (administratively down).
Protocol	States whether IP is enabled (up) or disabled (down) on the interface.

Example (brief)

```
FTOS#show ip int brief
Interface      IP-Address OK  Method Status
Protocol
TenGigEth 0/0  unassigned YES Manual up                    up
TenGigEth 0/1  unassigned YES Manual up                    up
...
TenGigEth 0/35 unassigned YES Manual up                    up
fortyGigE 0/48 unassigned NO  Manual up                    down
fortyGigE 0/52 unassigned NO  Manual administratively down down
fortyGigE 0/56 unassigned NO  Manual administratively down down
fortyGigE 0/60 unassigned NO  Manual administratively down down
ManagementE 0/0 10.1.1.1   YES Manual up                   up
ManagementE 1/0 unassigned NO  Manual up                   not
present
...
ManagementE 11/0 unassigned NO  Manual up                  not
present
Vlan 1         unassigned NO  Manual administratively down down
Vlan 1002      unassigned NO  Manual administratively down down
FTOS#
```

show ip management-route

View the IP addresses assigned to the Management interface.

S5000

Syntax

```
show ip management-route [all | connected | summary | static]
```

Parameters

all	(OPTIONAL) Enter the keyword `all` to view all IP addresses assigned to all Management interfaces on the switch.
connected	(OPTIONAL) Enter the keyword `connected` to view only routes directly connected to the Management interface.
summary	(OPTIONAL) Enter the keyword `summary` to view a table listing the number of active and non-active routes and their sources.
static	(OPTIONAL) Enter the keyword `static` to view non-active routes also.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip management-route

Destination     Gateway                    State
-----------     -------                    -----
10.1.2.0/24     ManagementEthernet 0/0     Connected
172.16.1.0/24   10.1.2.4                   Active
FTOS#
```

show ipv6 management-route

Display the IPv6 static routes configured for the management interface.

S5000

Syntax `show ipv6 management-route [all | connected | summary | static]`

Parameters

all	(OPTIONAL) Enter the keyword `all` to view all IP addresses assigned to all Management interfaces on the switch.
connected	(OPTIONAL) Enter the keyword `connected` to view only routes directly connected to the Management interface.
summary	(OPTIONAL) Enter the keyword `summary` to view a table listing the number of active and non-active routes and their sources.
static	(OPTIONAL) Enter the keyword `static` to view non-active routes also.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ipv6 management-route
IPv6 Destination   Gateway                  State
----------------    -------                 -----
2001:34::0/64      ManagementEthernet 0/0  Connected
2001:68::0/64      2001:34::16             Active
FTOS#
```

show ip protocols

View information on all routing protocols enabled and active on the switch.

S5000

Syntax	`show ip protocols`
Command Modes	- EXEC - EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
FTOS#show ip protocols
Routing Protocol is "bgp 1"
  Cluster Id is set to 20.20.20.3
  Router Id is set to 20.20.20.3
  Fast-external-failover enabled
  Regular expression evaluation optimization enabled
  Capable of ROUTE_REFRESH
  For Address Family IPv4 Unicast
   BGP table version is 0, main routing table version 0
   Distance: external 20 internal 200 local 200
   Neighbor(s):
     Address : 20.20.20.2
     Filter-list in : foo
     Route-map in : foo
     Weight : 0
   Address : 5::6
     Weight : 0
FTOS#
```

show ip route

View information, including how they were learned, about the IP routes on the switch.

S5000

Syntax

```
show ip route [ip-address] | [mask] | [longer-prefixes] | list
prefix-list | { protocol [process-id | routing-tag]}
{[ connected | all | static | summary]}
```

Parameters

ip-address	(OPTIONAL) Specify a name of a device or the IP address of the device to view more detailed information about the route.
mask	(OPTIONAL) Specify the network mask of the route. Use this parameter with the IP address parameter.
longer-prefixes	(OPTIONAL) Enter the keywords `longer-prefixes` to view all routes with a common prefix.

list *prefix-list*	(OPTIONAL) Enter the keyword `list` and the name of a configured prefix list. For more information, refer to the show ip route list command.
protocol	(OPTIONAL) Enter the name of a routing protocol (`bgp`, `isis`, `ospf`, `rip`) or the keywords `connected` or `static`. If you enter `ospf`, you can include the OSPF *`process-id`*
process-id	(OPTIONAL) Specify that only OSPF routes with a certain process ID must be displayed.
routing-tag	(OPTIONAL) Specify that only ISIS routes with a certain routing tag must be displayed.
connected	(OPTIONAL) Enter the keyword `connected` to view only the directly connected routes.
all	(OPTIONAL) Enter the keyword `all` to view both active and non-active routes.
static	(OPTIONAL) Enter the keyword `static` to view only routes configured by the `ip route` command.
summary	(OPTIONAL) Enter the keyword `summary`. For more information, refer to the show ip route summary command.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output for the `show ip route all` command in the Example below.

Field	Description
(undefined)	Identifies the type of route: • C = connected • S = static • R = RIP • B = BGP • IN = internal BGP • EX = external BGP • LO = Locally Originated • O = OSPF • IA = OSPF inter area • N1 = OSPF NSSA external type 1 • N2 = OSPF NSSA external type 2 • E1 = OSPF external type 1

- E2 = OSPF external type 2
- i = IS-IS
- L1 = IS-IS level-1
- L2 = IS-IS level-2
- IA = IS-IS inter-area
- * = candidate default
- > = non-active route
- + = summary routes

Destination	Identifies the route’s destination IP address
Gateway	Identifies whether the route is directly connected and on which interface the route is configured.
Dist/Metric	Identifies if the route has a specified distance or metric.
Last Change	Identifies when the route was last changed or configured.

Example

```
FTOS#show ip route all

Codes:C- connected, S - static, R - RIP
      B- BGP, IN - internal BGP, EX - external BGP, LO -
Locally Originated
      O- OSPF, IA - OSPF inter area N1 - OSPF NSSA external
type 1
      N2- OSPF NSSA external type 2, E1 - OSPF external type 1
      E2- OSPF external type 2, i - IS-IS, L1 - IS-IS level-1
      L2- IS-IS level-2, IA - IS-IS inter area, * - candidate
default
      >- non-active route + - summary route

Gateway of last resort is not set

     Destination     Gateway            Dist/Metric Last Change
----------- ------- ----------- -----------
R   3.0.0.0/8       via 100.10.10.10, So 2/8 120/1   00:07:12
                    via 101.10.10.10, So 2/9
    100.10.10.0/24  Direct, So 2/8           0/0     00:08:54
> R 100.10.10.0/24  Direct, So 2/8           120/0   00:08:54
C   101.10.10.0/24  Direct, So 2/9           0/0     00:09:15
> R 101.10.10.0/24  Direct, So 2/9           120/0   00:09:15
FTOS#
```

Example (Summary)

```
FTOS#show ip route summary

Route Source  Active Routes   Non-active Routes
connected     2               0
static        1               0
Total         3               0
Total 3 active route(s) using 612 bytes
R1_E600i>show ip route static ?
|                    Pipe through a command
<cr>
R1_E600i>show ip route static
    Destination   Gateway            Dist/Metric Last Change
----------- ------- ----------- -----------
```

```
*S  0.0.0.0/0     via 10.10.91.9, Te 1/2     1/0        3d2h
FTOS>
```

show ip route list

Display IP routes in an IP prefix list.

S5000

Syntax `show ip route list` *`prefix-list`*

Parameters

prefix-list	Enter the name of a configured prefix list.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip route list test

Codes:C- connected, S - static, R - RIP,
      B- BGP, IN - internal BGP, EX - external BGP,LO -
Locally Originated,
      O- OSPF, IA - OSPF inter area, N1 - OSPF NSSA external
type 1,
      N2- OSPF NSSA external type 2, E1 - OSPF external type 1,
      E2- OSPF external type 2, i - IS-IS, L1 - IS-IS level-1,
      L2- IS-IS level-2, IA - IS-IS inter area, * - candidate
default,
      >- non-active route, + - summary route

Gateway of last resort is not set

    Destination   Gateway              Dist/Metric Last Change
    -----------   -------              ----------- -----------
R   2.1.0.0/24   via 2.1.4.1, Te 4/43   120/2       3d0h
R   2.1.1.0/24   via 2.1.4.1, Te 4/43   120/2       3d1h
R   2.1.2.0/24   via 2.1.4.1, Te 4/43   120/1       3d0h
R   2.1.3.0/24   via 2.1.4.1, Te 4/43   120/1       3d1h
C   2.1.4.0/24   Direct, Te 4/43          0/0       3d1h
```

Related Commands

ip prefix-list – enters CONFIGURATION-IP PREFIX-LIST mode and configures a prefix list.

show ip prefix-list summary – displays a summary of the configured prefix lists.

show ip route summary

View a table summarizing the IP routes in the switch.

S5000

Syntax `show ip route summary`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip route summary` shown in the Example below.

Column Heading	Description
Route Source	Identifies how the route is configured in FTOS.
Active Routes	Identifies the best route if a route is learned from two protocol sources.
Non-active Routes	Identifies the back-up routes when a route is learned by two different protocols. If the best route or active route goes down, the non-active route becomes the best route.
ospf 100	If routing protocols (OSPF, RIP) are configured and routes are advertised, then information on those routes is displayed.
Total 1388 active...	Displays the number of active and non-active routes and the memory usage of those routes. If there are no routes configured in the FTOS, this line does not appear.

Example

```
FTOS>show ip route summary

Route Source   Active Routes   Non-active Routes
connected      17              0
static         3               0
ospf 100       1368            2
Intra-area: 762 Inter-area: 1 External-1: 600 External-2: 5
Total          1388            2
Total 1388 active route(s) using 222440 bytes
Total 2 non-active route(s) using 128 bytes
FTOS>
```

Related Commands

show ip route – displays information about the routes found in the switch.

show ip traffic

View IP, ICMP, UDP, TCP and ARP traffic statistics.

S5000

Syntax `show ip traffic`

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The following describes keywords in output for the `show ip traffic` command shown in the Example below.

Keyword	Definition
unknown protocol...	No receiver for these packets. Counts those packets whose protocol type field is not recognized by FTOS.
not a gateway...	Packets can not be routed; the host/network is unreachable.
security failures...	Counts the number of received unicast/multicast packets that could not be forwarded due to: • route not found for unicast/multicast; ingress interfaces do not belong to the destination multicast group • destination IP address belongs to reserved prefixes; the host/ network is unreachable
bad options...	Unrecognized IP option on a received packet.
Frags:	IP fragments received.
... reassembled	Number of IP fragments that were reassembled.
... timeouts	Number of times a timer expired on a reassembled queue.
... too big	Number of invalid IP fragments received.
... couldn’t fragment	Number of packets that could not be fragmented and forwarded.
...encapsulation failed	Counts those packets which could not be forwarded due to ARP resolution failure. FTOS sends an arp request prior to forwarding an IP packet. If a reply is not received, FTOS repeats the request three times. These packets are counted in encapsulation failed.
Rcvd:	
...short packets	The number of bytes in the packet are too small.
...bad length	The length of the packet was not correct.
...no port broadcasts	The incoming broadcast/multicast packet did not have any listener.

...socket full	The applications buffer was full and the incoming packet had to be dropped.

The F10 Monitoring MIB provides access to the statistics described below.

- **IP Statistics: Bcast: Received:** Object = f10BcastPktRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.1
- **IP Statistics: Bcast: Sent:** Object = f10BcastPktSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.2
- **IP Statistics: Mcast: Received:** Object = f10McastPktRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.3
- **IP Statistics: Mcast: Sent:** Object = f10McastPktSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.4
- **ARP Statistics: Rcvd: Request:** Object = f10ArpReqRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.1
- **ARP Statistics: Rcvd: Replies:** Object = f10ArpReplyRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.3
- **ARP Statistics: Sent: Request:** Object = f10ArpReqSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.2
- **ARP Statistics: Sent: Replies:** Object = f10ArpReplySent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.4
- **ARP Statistics: Sent: Proxy:** Object = f10ArpProxySent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.5

Example

```
FTOS#show ip traffic
Control Processor IP Traffic:

IP statistics:
  Rcvd: 23857 total, 23829 local destination
    0 format errors, 0 checksum errors, 0 bad hop count
    0 unknown protocol, 0 not a gateway
    0 security failures, 0 bad options
  Frags: 0 reassembled, 0 timeouts, 0 too big
    0 fragmented, 0 couldn't fragment
  Bcast: 28 received, 0 sent; Mcast: 0 received, 0 sent
  Sent: 16048 generated, 0 forwarded
    21 encapsulation failed, 0 no route
ICMP statistics:
  Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0
unreachable
    0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0
quench
    0 parameter, 0 timestamp, 0 info request, 0 other
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
    0 mask requests, 0 mask replies, 0 quench, 0 timestamp
    0 info reply, 0 time exceeded, 0 parameter problem
UDP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
    0 short packets, 0 bad length, 0 no port broadcasts, 0
socket full
  Sent: 0 total, 0 forwarded broadcasts
TCP statistics:
  Rcvd: 23829 total, 0 checksum errors, 0 no port
  Sent: 16048 total
ARP statistics:
  Rcvd: 156 requests, 11 replies
  Sent: 21 requests, 10 replies (0 proxy)
Routing Processor1 IP Traffic:
```

show tcp statistics

View information on TCP traffic through the switch.

S5000

Syntax	`show tcp statistics`
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	The following describes the `show tcp statistics` command shown in the Example below.

Field	Description
Rcvd:	Displays the number and types of TCP packets received by the switch. • Total = total packets received • no port = number of packets received with no designated port
0 checksum error...	Displays the number of packets received with the following: • checksum errors • bad offset to data • too short
1888 packets...	Displays the number of packets and bytes received in sequence.
17 dup...	Displays the number of duplicate packets and bytes received.
0 partially...	Displays the number of partially duplicated packets and bytes received.
7 out-of-order...	Displays the number of packets and bytes received out of order.
0 packets with data after window	Displays the number of packets and bytes received that exceed the switch's window size.
0 packets after close	Displays the number of packet received after the TCP connection was closed.
0 window probe packets...	Displays the number of window probe and update packets received.
41 dup ack...	Displays the number of duplicate acknowledgement packets and acknowledgement packets with data received.
10184 ack...	Displays the number of acknowledgement packets and bytes received.
Sent:	Displays the total number of TCP packets sent and the number of urgent packets sent.

25 control packets...	Displays the number of control packets sent and the number retransmitted.
11603 data packets...	Displays the number of data packets sent.
24 data packets retransmitted	Displays the number of data packets resent.
355 ack..	Displays the number of acknowledgement packets sent and the number of packet delayed.
0 window probe...	Displays the number of window probe and update packets sent.
0 Connections initiated...	Displays the number of TCP connections initiated, accepted, and established.
15 Connections closed...	Displays the number of TCP connections closed, dropped.
12 Total rxmt...	Displays the number of times the switch tried to re-send data and the number of connections dropped during the TCP retransmit timeout period.
0 Keepalive....	Lists the number of keepalive packets in timeout, the number keepalive probes and the number of TCP connections dropped during keepalive.

Example

```
FTOS#show tcp stat
Rcvd: 10585 Total, 0 no port
   0 checksum error, 0 bad offset, 0 too short
   329 packets (1263 bytes) in sequence
   17 dup packets (6 bytes)
   0 partially dup packets (0 bytes)
   7 out-of-order packets (0 bytes)
   0 packets ( 0 bytes) with data after window
   0 packets after close
   0 window probe packets, 41 window update packets
   41 dup ack packets, 0 ack packets with unsend data
   10184 ack packets (12439508 bytes)
Sent: 12007 Total, 0 urgent packets
   25 control packets (including 24 retransmitted)
   11603 data packets (12439677 bytes)
   24 data packets (7638 bytes) retransmitted
   355 ack only packets (41 delayed)
   0 window probe packets, 0 window update packets
0 Connections initiated, 15 connections accepted, 15
connections established
15 Connections closed (including 14 dropped, 0 embryonic
dropped)
12 Total rxmt timeout, 1 connections dropped in rxmt timeout
0 Keepalive timeout, 0 keepalive probe, 0 Connections dropped
in keepalive
FTOS#
```

Related Commands

show ip cam stack-unit – displays the CAM table.

24

IPv6 Access Control Lists (IPv6 ACLs)

IPv6 ACLs and IPv6 Route Map commands are supported on the Dell Networking S5000 switch.

This chapter contains the following sections

- IPv6 ACL Commands
- IPv6 Route Map Commands

NOTE: For IPv4 ACL commands, refer to the Access Control Lists (ACL) chapter.

Important Points to Remember

- The S5000 requires manual CAM usage space allotment. For more information, refer to the cam-acl command.
- Egress IPv6 ACL and IPv6 ACL on the Loopback interface is not supported.
- Reference to an empty ACL permits any traffic.
- ACLs are not applied to self-originated traffic (for example, Control Protocol traffic not affected by IPv6 ACL because the routed bit is not set for Control Protocol traffic and for egress ACLs the routed bit must be set).
- You can use the same access list name for both IPv4 and IPv6 ACLs.
- You can apply both IPv4 and IPv6 ACLs on an interface at the same time.
- You can apply IPv6 ACLs on physical interfaces and a logical interfaces (Port-channel/VLAN).
- Non-contiguous masks are not supported in source or destination addresses in IPv6 ACL entries.
- Because the prefix mask is specified in /x format in IPv6 ACLs, inverse mask is not supported.

IPv6 ACL Commands

The following commands configure IPv6 ACLs.

cam-acl

Allocate space for IPv6 ACLs.

S5000

Syntax

```
cam-acl {default | l2acl 1-10 ipv4acl 1-10 ipv6acl 0-10 ipv4qos
1-10 l2qos 1-10}
```

Parameters

default	Use the default CAM profile settings, and set the CAM as follows: • L3 ACL (ipv4acl): **6** • L2 ACL(l2acl): **5** • IPv6 L3 ACL (ipv6acl): **0** • L3 QoS (ipv4qos): **1** • L2 QoS (l2qos): **1**
l2acl ***1-10*** **ipv4acl** ***1-10*** **ipv6acl** ***0-10*** **ipv4qos** ***1-10*** **l2qos** ***1-10***	Allocate space to support IPv6 ACLs. You must enter all of the profiles and a range. Enter the CAM profile name followed by the amount to be allotted. The total space allocated must equal 13. The `ipv6acl` range must be a factor of 2.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

For the new settings to take effect, you must save the new CAM settings to the startup-config (`write-mem` or `copy run start`), then reload the system.

The total amount of space allowed is 16 FP Blocks. System flow requires three blocks and these cannot be reallocated.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

Ranges for the CAM profiles are 1-10, except for the `ipv6acl profile` which is 0-10. The ipv6acl allocation must be a factor of 2 (2, 4, 6, 8, 10).

cam-acl-egress

Allocate space for IPv6 egress ACLs.

S5000

Syntax `cam-acl-egress {default | l2acl 1-4 ipv4acl 1-4 ipv6acl 0-4}`

Parameters

default	Use the default CAM profile settings, and set the CAM as follows: • L2 ACL(l2acl): **1** • L3 ACL (ipv4acl: **1** • IPv6 L3 ACL (ipv6acl): **2**
l2acl ***1-4*** **ipv4acl** ***1- 4*** **ipv6acl** ***0-4***	Allocate space to support IPv6 ACLs. You must enter all of the profiles and a range. Enter the CAM profile name followed by the amount to be allotted. The total space allocated must equal 13. The `ipv6acl` range must be a factor of 2.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

For the new settings to take effect, you must save the new CAM settings to the startup-config (`write-mem` or `copy run start`), then reload the system.

The total amount of space allowed is 16 FP Blocks. System flow requires three blocks and these cannot be reallocated.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

Ranges for the CAM profiles are 1-10, except for the `ipv6acl profile` which is 0-10. The ipv6acl allocation must be a factor of 2 (2, 4, 6, 8, 10).

Example

```
FTOS#
FTOS#configure
FTOS(conf)#cam-acl-egress ?
default      Reset Egress CAM ACL entries to default setting
l2acl        Set L2-ACL entries
FTOS(conf)#cam-acl-egress l2acl ?
<1-4>        Number of FP blocks for l2acl
FTOS(conf)#cam-acl-egress l2acl 1 ?
ipv4acl      Set IPV4-ACL entries
FTOS(conf)#cam-acl-egress l2acl 1 ipv4acl 1 ?
ipv6acl      Set IPV6-ACL entries
FTOS(conf)#cam-acl-egress l2acl 1 ipv4acl 1 ipv6acl ?
<0-4>        Number of FP blocks for IPV6 (multiples of 2)
FTOS(conf)#cam-acl-egress l2acl 1 ipv4acl 1 ipv6acl 2
```

clear counters ipv6 access-group

Erase all counters maintained for the IPv6 access lists.

S5000

Syntax `clear counters ipv6 access-group [access-list-name]`

Parameters

access-list-name	(OPTIONAL) Enter the name of a configured access-list, up to 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

deny

Configure a filter that drops IPv6 packets that match the filter criteria.

S5000

Syntax

`deny {ipv6-protocol-number | icmp | ipv6 | tcp | udp}`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no deny {ipv6-protocol-number | icmp | ipv6 | tcp | udp}` command

Parameters

ip-protocol-number	Enter an IPv6 protocol number. The range is 0 to 255.
icmp	Enter the keyword `icmp` to deny internet control message protocol (ICMP) version 6.
ipv6	Enter the keyword `ipv6` to deny any internet protocol (IP) version 6.
tcp	Enter the keyword `tcp` to deny the Transmission Control Protocol.
udp	Enter the keyword `udp` to deny the User Datagram Protocol.

Defaults Not configured.

Command Modes ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

deny icmp

Configure a filter to drop all or specific ICMP messages.

S5000

Syntax

```
deny icmp {source address mask | any | host ipv6-address}
{destination address | any | host ipv6-address} [count [byte]]
| [log] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no deny icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword `host` followed by the IPv6 address of the host in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zero. Only one occurrence of this notation is permitted in an IPv6 address.
destination address	Enter the IPv6 address of the network or host to which the packets are sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword `log` to have the information kept in an ACL log file.
monitor	(OPTIONAL) Enter the keyword `monitor` to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The information below lists the keywords displayed in the CLI help and their corresponding ICMP Message Type Name.

Table 7. Keywords for ICMP Message Type Names

Keyword	ICMP Message Type Name
dest-unreachable	Destination unreachable.
echo	Echo request (ping).
echo-reply	Echo reply.
inverse-nd-na	Inverse neighbor discovery advertisement.
inverse-nd-ns	Inverse neighbor discovery solicitation.

Keyword	ICMP Message Type Name
log	Log matches against this entry.
mobile-advertisement	Mobile prefix advertisement.
mobile-solicitation	Mobile prefix solicitation.
mrouter-advertisement	Multicast router advertisement.
mrouter-solicitation	Multicast router solicitation.
mrouter-termination	Multicast router termination.
nd-na	Neighbor advertisement.
nd-ns	Neighbor solicitation.
packet-too-big	Packet is too big.
parameter-problem	Parameter problems.
redirect	Neighbor redirect.
router-advertisement	Neighbor discovery router advertisement.
router-renumbering	All routers renumbering.
router-solicitation	Neighbor discovery router solicitation.
time-exceeded	All time exceeded.

deny tcp

Configure a filter that drops TCP packets that match the filter criteria.

S5000

Syntax

```
deny tcp {source address mask | any | host ipv6-address}
[operator port [port]] {destination address | any | host ipv6-
address} [bit] [operator port [port]] [count [byte]] |
[monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no deny tcp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.

mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword `host` followed by the IPv6 address of the host in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zero. Only one occurrence of this notation is permitted in an IPv6 address.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the port command parameter).
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination address	Enter the IPv6 address of the network or host to which the packets are sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
bit	Enter a flag or combination of bits: • `ack:` acknowledgement field • `fin:` finish (no more data from the user) • `psh:` push function • `rst:` reset the connection • `syn:` synchronize sequence numbers • `urg:` urgent field
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.

monitor	(OPTIONAL) Enter the keyword `monitor` to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (`gt`, `lt`, `range`) may require more than one entry. The range of ports is configured in the CAM based on bitmask boundaries; the space required depends on exactly what ports are included in the range.

Example An ACL rule with a TCP port range of 4000 - 8000 uses eight entries in the CAM:

```
Rule#    Data           Mask         From   To  #Covered

1   0000111110100000 1111111111100000 4000  4031  32
2   0000111111000000 1111111111000000 4032  4095  64
3   0001000000000000 1111100000000000 4096  6143  2048
4   0001100000000000 1111110000000000 6144  7167  1024
5   0001110000000000 1111111000000000 7168  7679  512
6   0001111000000000 1111111100000000 7680  7935  256
7   0001111100000000 1111111111000000 7936  7999  64
8   0001111101000000 1111111111111111 8000  8000  1

Total Ports: 4001
```

Example An ACL rule with TCP port `lt 1023` takes only one entry in the CAM:

```
Rule#    Data            Mask         From  To    #Covered

1   0000000000000000 1111110000000000 0     1023    1024

Total Ports: 1024
```

Related Commands

deny – assigns a filter to deny IP traffic.

deny udp – assigns a filter to deny UDP traffic.

deny udp

Configure a filter to drop user datagram protocol (UDP) packets meeting the filter criteria.

S5000

Syntax

```
deny udp {source address mask | any | host ipv6-address}
[operator port [port]] {destination address | any | host ipv6-
address} [operator port [port]] [count [byte]] | [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no deny udp {`*`source address mask`*` | any | host `*`ipv6-address`*`} {`*`destination address`*` | any | host `*`ipv6-address`*`}` command

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword `host` followed by the IPv6 address of the host in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zero.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the port command parameter).
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is 0 to 65535.
destination address	Enter the IPv6 address of the network or host to which the packets are sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
monitor	(OPTIONAL) Enter the keyword `monitor` to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (`gt`, `lt`, `range`) may require more than one entry. The range of ports is configured in the CAM based on bitmask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range of 4000 - 8000 uses eight entries in the CAM:

```
Rule#    Data           Mask         From   To  #Covered

1   0000111110100000 1111111111100000 4000   4031  32
2   0000111111000000 1111111111000000 4032   4095  64
3   0001000000000000 1111100000000000 4096   6143  2048
4   0001100000000000 1111110000000000 6144   7167  1024
5   0001110000000000 1111111000000000 7168   7679  512
6   0001111000000000 1111111100000000 7680   7935  256
7   0001111100000000 1111111111000000 7936   7999  64
8   0001111101000000 1111111111111111 8000   8000  1

Total Ports: 4001
```

Example

An ACL rule with TCP port `lt 1023` takes only one entry in the CAM:

```
Rule#    Data            Mask         From   To    #Covered

1   0000000000000000 1111110000000000 0      1023    1024

Total Ports: 1024
```

Related Commands

deny – assigns a filter to deny IP traffic.

deny tcp – assigns a deny filter for TCP traffic.

ipv6 access-group

Assign an IPv6 access-group to an interface.

S5000

Syntax

`ipv6 access-group` *`access-list-name`* `{in | out} [implicit-permit] [vlan` *`range`*`]`

To delete an IPv6 access-group configuration, use the `no ipv6 access-group` *`access-list-name`* `{in} [implicit-permit] [vlan` *`range`*`]` command.

Parameters

access-list-name	Enter the name of a configured access list, up to 140 characters.
in | out	Enter either the keyword `in` or `out` to apply the IPv6 ACL to incoming traffic (ingress) or outgoing traffic (egress).
implicit-permit	(OPTIONAL) Enter the keywords `implicit-permit` to change the default action of the IPv6 ACL from implicit-deny to implicit-permit (that is, if the traffic does not match the filters in the IPv6 ACL, the traffic is permitted instead of dropped).

vlan *range*	(OPTIONAL) Enter the keyword `vlan` followed by the VLAN range in a comma separated format. The range is 1 to 4094.

Defaults Disabled.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information You can assign an IPv6 access group to a physical, LAG, or VLAN interface context.

Example

```
FTOS(conf-if-te-9/0)#ipv6 access-group AclList1 in implicit-
permit vlan 10-20

FTOS(conf-if-te-9/0)#show config
!
interface TenGigabitEthernet 9/0
  no ip address
  ipv6 access-group AclList1 in implicit-permit Vlan 10-20
  no shutdown
FTOSconf-if-te-9/0)#
```

ipv6 control-plane egress-filter

Enable egress Layer 3 ACL lookup for IPv6 CPU traffic.

S5000

Syntax `ipv6 control-plane egress-filter`

Defaults Not enabled.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

ipv6 access-list

Configure an access list based on IPv6 addresses or protocols.

S5000

Syntax `ipv6 access-list` *`access-list-name`*

To delete an access list, use the `no ipv6 access-list` *`access-list-name`* command.

Parameters

access-list-name	Enter the as the access list name as a string, up to 140 characters.

Defaults All access lists contain an implicit “deny any”; that is, if no match occurs, the packet is dropped.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The number of entries allowed per ACL is hardware-dependent. For detailed specification on entries allowed per ACL, refer to your switch ocumentation.

Related Commands show config – views the current configuration.

permit

Select an IPv6 protocol number, ICMP, IPv6, TCP, or UDP to configure a filter that match the filter criteria.

S5000

Syntax

```
permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp}
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number
- Use the `no permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp}` command

Parameters

ip-protocol-number	Enter an IPv6 protocol number. The range is 0 to 255.
icmp	Enter the keyword `icmp` to filter internet control message protocol (ICMP) version 6.
ipv6	Enter the keyword `ipv6` to filter any iInternet protocol (IP) version 6.
tcp	Enter the keyword `tcp` to filter the Transmission Control Protocol.
udp	Enter the keyword `udp` to filter the User Datagram Protocol.

Defaults Not configured.

Command Modes ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

permit icmp

Configure a filter to allow all or specific internet control message protocol (ICMP) messages.

S5000

Syntax

`permit icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address} [message-type] [count [byte]] | [log] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command.

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (/x).
host *ipv6-address*	Enter the keyword `host` followed by the IPv6 address of the host in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zero.
destination address	Enter the IPv6 address of the network or host to which the packets are sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
message-type	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type. The range is 0 to 255 for ICMP type and 0 to 255 for ICMP code.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword `log` to have the information kept in an ACL log file.
monitor	(OPTIONAL) Enter the keyword `monitor` to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes ACCESS-LIST

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

permit tcp

Configure a filter to pass TCP packets that match the filter criteria.

S5000

Syntax

`permit tcp {[`*`source address`*` | `*`mask`*` ]} [any] {[ host `*`ipv6-address`*` | [`*`operator`*` ][`*`port port`*`] | [`*`destination address`*` ] | [ `*`bit`*` ]} [count] | [byte] | [log] | [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `permit tcp {[source address | mask ]} [any] {[ host ipv6-address | [operator ] | [port port] | [destination address ] | [ bit ]} [count] | [byte] | [log] | [monitor]` command.

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword `host` followed by the IPv6 address of the host in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zero.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two port for the port parameter.)
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet

- 20 and 21 = FTP
- 25 = SMTP
- 169 = SNMP

destination address	Enter the IPv6 address of the network or host to which the packets are sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
bit	Enter a flag or combination of bits: - `ack`: acknowledgement field - `fin`: finish (no more data from the user) - `psh`: push function - `rst`: reset the connection - `syn`: synchronize sequence numbers - `urg`: urgent field
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword `log` to have the information kept in an ACL log file.
monitor	(OPTIONAL) Enter the keyword `monitor` to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (`gt`, `lt`, `range`) may require more than one entry. The range of ports is configured in the CAM based on bitmask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range 4000 - 8000 uses eight entries in the CAM:

```
Rule# Data             Mask             From   To  #Covered

1 0000111110100000  1111111111100000  4000  4031   32
2 0000111111000000  1111111111000000  4032  4095   64
3 0001000000000000  1111100000000000  4096  6143   2048
4 0001100000000000  1111110000000000  6144  7167   1024
5 0001110000000000  1111111000000000  7168  7679   512
6 0001111000000000  1111111100000000  7680  7935   256
7 0001111100000000  1111111111000000  7936  7999   64
8 0001111101000000  1111111111111111  8000  8000   1
```

```
Total Ports: 4001
```

Example

An ACL rule with a TCP port `lt 1023` takes only one entry in the CAM:

```
Rule#  Data             Mask             From  To #Covered

1  0000000000000000 1111110000000000 0    1023  1024

Total Ports: 1024
```

Related Commands

permit – assigns a permit filter for IP packets.

permit udp – assigns a permit filter for UDP packets.

permit udp

Configure a filter to pass UDP packets meeting the filter criteria.

S5000

Syntax

`permit udp {source address mask | any | host ipv6-address} [operator port [port]] {destination address | any | host ipv6-address} [operator port [port]] [count [byte]] | [log] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit udp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command.

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword `host` followed by the IPv6 address of the host in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zero.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to

- `gt` = greater than
- `lt` = less than
- `range` = inclusive range of ports (you must specify two port for the port parameter.)

port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is 0 to 65535.
destination address	Enter the IPv6 address of the network or host to which the packets are sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword `log` to have the information kept in an ACL log file.
monitor	(OPTIONAL) Enter the keyword `monitor` to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (`gt`, `lt`, `range`) may require more than one entry. The range of ports is configured in the CAM based on bitmask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range 4000 - 8000 uses eight entries in the CAM:

```
Rule# Data            Mask            From  To   #Covered

1 0000111110100000  1111111111100000  4000  4031   32
2 0000111111000000  1111111111000000  4032  4095   64
3 0001000000000000  1111100000000000  4096  6143   2048
4 0001100000000000  1111110000000000  6144  7167   1024
5 0001110000000000  1111111000000000  7168  7679   512
6 0001111000000000  1111111100000000  7680  7935   256
7 0001111100000000  1111111111000000  7936  7999   64
8 0001111101000000  1111111111111111  8000  8000   1

Total Ports: 4001
```

Example

An ACL rule with a TCP port `lt 1023` takes only one entry in the CAM:

```
Rule#  Data            Mask         From  To #Covered

1  0000000000000000 1111110000000000 0   1023  1024
```

```
Total Ports: 1024
```

Related Commands

permit – assigns a permit filter for IP packets.

permit tcp – assigns a permit filter for TCP packets.

remark

Enter a description for an IPv6 ACL entry.

S5000

Syntax

`remark` *`remark number`* `[`*`description`*`]`

To delete the description, use the `no remark` *`remark number`* command (it is not necessary to include the remark description that you are deleting).

Parameters

remark number	Enter the remark number. The range is 0 to 4294967290. **NOTE:** You can use the same sequence number for the remark and an ACL rule.
description	Enter a description of up to 80 characters.

Defaults

Not configured.

Command Modes

ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

As shown in the Example below, the same sequence number is used for the remark and an ACL rule. The remark precedes the rule in the running-configuration because it is assumed that the remark is for that rule or that group of rules that follow the remark. You can configure up to 4294967290 remarks in a given ACL.

Example

```
FTOS(config-ipv6-acl)#remark 10 Remark for Entry # 10
FTOS(config-ipv6-acl)#show config
!
ipv6 access-list Acl1
  description IPV6 Access-list
  seq 5 permit ipv6 1111::2222/127 host 3333::1111 log count
bytes
  remark 10 Remark for Entry # 10
  seq 10 permit icmp host 3333:: any mobile-advertisement log
  seq 15 deny tcp any any rst
  seq 20 permit udp any any gt 100 count
!FTOS(config-ipv6-acl)#
```

Related Commands

show config – displays the current ACL configuration.

resequence access-list

Re-assign sequence numbers to entries of an existing access-list.

S5000

Syntax

```
resequence access-list {ipv4 | ipv6 | mac} {access-list-name
StartingSeqNum Step-to-Increment}
```

Parameters

ipv4 | ipv6 | mac	Enter the keyword `ipv4, ipv6` or `mac` to identify the access list type to resequence.
access-list-name	Enter the name of a configured IP access list, up to 140 characters.
StartingSeqNum	Enter the starting sequence number to resequence. The range is 0 to 4294967290.
Step-to-Increment	Enter the step to increment the sequence number. The range is 1 to 4294967290.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information When all sequence numbers have been exhausted, this feature permits re-assigning new sequence number to entries of an existing access-list.

Related Commands resequence prefix-list ipv6 – resequences a prefix list.

resequence prefix-list ipv6

Re-assign sequence numbers to entries of an existing prefix list.

S5000

Syntax

```
resequence prefix-list ipv6 {prefix-list-name StartingSeqNum
Step-to-increment}
```

Parameters

prefix-list-name	Enter the name of configured prefix list, up to 140 characters. Increased the name string to accept up to 140 characters.
StartingSeqNum	Enter the starting sequence number to resequence. The range is 0 to 65535.

Step-to-Increment	Enter the step to increment the sequence number. The range is 1 to 65535.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information When all sequence numbers have been exhausted, this feature permits re-assigning new sequence number to entries of an existing access-list.

Related Commands resequence access-list – resequences an access-list.

seq

Assign a sequence number to a deny or permit the filter in an IPv6 access list while creating the filter.

S5000

Syntax

```
seq sequence-number {deny | permit} {ipv6-protocol-number |
icmp | ip | tcp | udp} {source address mask | any | host ipv6-
address} {destination address | any | host ipv6-address}
[operator port [port]] [count [byte]] | [monitor]
```

To delete a filter, use the `no seq sequence-number` command.

Parameters

sequence-number	Enter a number from 0 to 4294967290.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
ipv6-protocol-number	Enter an IPv6 protocol number. The range is 0 to 255.
icmp	Enter the keyword `icmp` to configure an internet control message protocol (ICMP) version 6 filter.
ipv6	Enter the keyword `ipv6` to configure any internet protocol (IP) version 6 filter.
tcp	Enter the keyword `tcp` to configure a Transmission Control Protocol filter.

udp	Enter the keyword `udp` to configure a User Datagram Protocol filter.
source address	Enter the IPv6 address of the network or host from which the packets were sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword `host` followed by the IPv6 address of the host in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zero.
operator	(OPTIONAL) Enter one of the following logical operands: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the port parameter.)
port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination address	Enter the IPv6 address of the network or host to which the packets are sent in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
message-type	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type . The range is 0 to 255 for ICMP type and 0 to 255 for ICMP code.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
monitor	(OPTIONAL) Enter the keyword `monitor` to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

deny – configures a filter to drop packets.

permit – configures a filter to forward packets.

show cam-acl

Show space allocated for IPv6 ACLs.

S5000

Syntax `show cam-acl`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show cam-acl

-- Chassis Cam ACL --
             Current Settings(in block sizes)
L2Acl        :         2
Ipv4Acl      :         4
Ipv6Acl      :         0
Ipv4Qos      :         2
L2Qos        :         1
L2PT         :         0
IpMacAcl     :         0
VmanQos      :         0
VmanDualQos  :         0
EcfmAcl      :         0
FcoeAcl      :         2
iscsiOptAcl  :         2

-- Stack unit 0 --
           Current Settings(in block sizes)
L2Acl        :         2
Ipv4Acl      :         4
Ipv6Acl      :         0
Ipv4Qos      :         2
L2Qos        :         1
L2PT         :         0
IpMacAcl     :         0
VmanQos      :         0
VmanDualQos  :         0
EcfmAcl      :         0
```

```
FcoeAcl      :          2
iscsiOptAcl  :          2
```

Related Commands

cam-acl – configures CAM profiles to support IPv6 ACLs.

show cam-acl-egress

Show information on FP groups allocated for egress ACLs.

S5000

Syntax `show cam-acl-egress`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show cam-acl-egress

-- Chassis Egress Cam ACL --
         Current Settings(in block sizes)
L2Acl   :        1
Ipv4Acl :        1
Ipv6Acl :        2

-- Stack unit 0 --
         Current Settings(in block sizes)
L2Acl   :        1
Ipv4Acl :        1
Ipv6Acl :        2

FTOS#show cam-acl
```

Related Commands

cam-acl – configures CAM profiles to support IPv6 ACLs.

show config

View the current IPv6 ACL configuration.

S5000

Syntax `show config`

Command Modes	ACCESS-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-ipv6-acl)#show config
!
ipv6 access-list Acl1
  seq 5 permit ipv6 1111::2222/127 host 3333::1111 log count 
bytes
  seq 10 permit icmp host 3333:: any mobile-advertisement log
  seq 15 deny tcp any any rst
  seq 20 permit udp any any gt 100 count
FTOS(conf-ipv6-acl)#
```

show ipv6 accounting access-list

View the IPv6 access-lists created on the S5000 and the sequence of filters.

S5000

Syntax

```
show ipv6 accounting {access-list access-list-name | cam_count}
interface type slot/port
```

Parameters

access-list-name	Enter the name of the ACL to be displayed, up to 140 characters.
cam_count	List the count of the CAM rules for this ACL.
interface *type slot/port*	Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Field	Description
“Ingress IPv6…”	Displays the name of the IPv6 ACL, in this Example “AclList1”.
“seq 10…”	Displays the filter. If the keywords `count` or `byte` were configured in the filter, the number of packets or bytes processed by the filter is displayed at the end of the line.

Example

```
FTOS#show ipv6 accounting access-list
!
Ingress IPv6 access list AclList1 on TenGigabitEthernet 9/0
Total cam count 15
  seq 10 permit icmp host 3333:: any mobile-advertisement log
  seq 15 deny tcp any any rst
  seq 20 permit udp any any gt 101 count (0 packets)
!
FTOS#
```

show running-config acl

Display the ACL running configuration.

S5000

Syntax `show running-config acl`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show running-config acl
!
ip access-list extended ext-acl1
!
ip access-list standard std-acl1
!
ipv6 access-list Acl1
description IPV6 Access-list
seq 5 permit ipv6 1111::2222/127 host 3333::1111 log count
bytes
remark 10 Remark for Entry # 10
  seq 10 permit icmp host 3333:: any mobile-advertisement log
  seq 15 deny tcp any any rst
  seq 20 permit udp any any gt 100 count
!FTOS#
```

test cam-usage

Verify that enough ACL CAM space is available for the IPv6 ACLs you have created.

S5000

Syntax `test cam-usage service-policy input`*`input-policy—map name`*

Parameters

input policy-map name	Enter the name of the policy-map to verify.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command applies to both IPv4 and IPv6 CAM Profiles, but is best used when verifying QoS optimization for IPv6 ACLs.

QoS Optimization for IPv6 ACLs does not impact the CAM usage for applying a policy on a single (or the first of several) interfaces. It is most useful when a policy is applied across multiple interfaces; it can reduce the impact to CAM usage across subsequent interfaces.

The following describes output for the `test cam-usage` command shown in the Example below.

Stack-unit	Lists the stack-unit(s) that are checked. Entering `all` shows the status for stack-units.
Portpipe	Lists the portpipe (port-set) or port pipes (port-sets) that are checked. Entering `all` shows the status for stack-units and port-pipes in the chassis.
CAM Partition	Shows the CAM profile of the CAM.
Available CAM	Identifies the amount of CAM space remaining for that profile.
Estimated CAM per Port	Estimates the amount of CAM space the listed policy requires.
Status	Indicates whether or not the policy is allowed in the CAM

Example

```
FTOS#test cam-usage service-policy input pmap_12 stack-unit all

Stack-| Portpipe| CAM Partn| Avail CAM| Est CAM/Port| Status
unit
--------------------------------------------------------------
 2|       1|       IPv4Flow|   232|         0|           Allowed
 2|       1|       IPv6Flow|     0|         0|           Allowed
 4|       0|       IPv4Flow|   232|         0|           Allowed
 4|       0|       IPv6Flow|     0|         0|           Allowed
FTOS#

FTOS#test cam-usage service-policy input pmap_12 stack-unit 4
port-set 0
Stack-| Portpipe| CAM Partn| Avail CAM| Est CAM/Port| Status
```

```
unit
----------------------------------------------------------------
 4|       0|        IPv4Flow|  232|         0|           Allowed
 4|       0|        IPv6Flow|    0|         0|           Allowed
FTOS#

FTOS#test cam-usage service-policy input pmap_12 stack-unit 2
port-set 1
Stack-| Portpipe| CAM Partn| Avail CAM| Est CAM/Port| Status
unit
-----------------------------------------------------------------
 2|        1|       IPv4Flow|  232|         0|            Allowed
 2|        1|       IPv6Flow|    0|         0|            Allowed
FTOS#
```

IPv6 Route Map Commands

The following commands allow you to configure route maps and their redistribution criteria.

match ipv6 address

Configure a filter to match routes based on IPv6 addresses specified in an access list.

S5000

Syntax

`match ipv6 address prefix-list-name`

To delete a match, use the `no match ipv6 address prefix-list-name` command.

Parameters

prefix-list-name	Enter the name of IPv6 prefix list, up to 140 characters.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

match ipv6 next-hop – redistributes routes that match the next-hop IP address.

match ipv6 route-source – redistributes routes that match routes advertised by other routers.

match ipv6 next-hop

Configure a filter which matches based on the next-hop IPv6 addresses specified in the IPv6 prefix list.

S5000

Syntax

`match ipv6 next-hop prefix-list` *`prefix-list-name`*

To delete a match, use the `no match ipv6 next-hop prefix-list` *`prefix-list-name`* command.

Parameters

prefix-list ***prefix-list-name***	Enter the keywords `prefix-list` followed by the name of configured prefix list, up to 140 characters.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

match ipv6 address – redistributes routes that match an IP address.

match ipv6 route-source – redistributes routes that match routes advertised by other routers.

match ipv6 route-source

Configure a filter which matches based on the routes advertised in the IPv6 prefix lists.

S5000

Syntax

`match ipv6 route-source prefix-list` *`prefix-list-name`*

To delete a match, use the `no match ipv6 route-source prefix-list` *`prefix-list-name`* command.

Parameters

prefix-list ***prefix-list-name***	Enter the keywords `prefix-list` followed by the name of configured prefix list, up to 140 characters.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

match ipv6 address – redistributes routes that match an IP address.

match ipv6 next-hop – redistributes routes that match the next-hop IP address.

route-map

Designate a IPv6 route map name and enter ROUTE-MAP mode.

S5000

Syntax	`route-map` *`map-name`* To delete a route map, use the `no route-map` *`map-name`* command.
Parameters	***map-name*** Enter a text string to name the route map, up to 140 characters.
Defaults	Not configured.
Command Modes	ROUTE-MAP
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
FTOS(conf)#route-map Rmap1

FTOS(config-route-map)#match ?
…
ip IP specific information
ipv6 IPv6 specific information
…
```

Related Commands

show config – views the current configuration.

set ipv6 next-hop

Configure a filter that specifies IPv6 address as the next hop.

S5000

Syntax	`set ipv6 next-hop` *`ipv6-address`* To delete the setting, use the `no set ipv6 next-hop` *`ipv6-address`* command.
Parameters	***ipv6-address*** Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
Defaults	Not configured.
Command Modes	ROUTE-MAP
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Usage Information	The `set ipv6 next-hop` command is the only way to set an IPv6 Next-Hop.

show config

View the current route map configuration.

S5000

Syntax	`show config`
Command Modes	ROUTE-MAP
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
FTOS(config-route-map)#show config
!
route-map Rmap1 permit 10
  match ip address v4plist
  match ipv6 address plist1
  match ipv6 next-hop prefix-list plist2
  match ipv6 route-source prefix-list plist3
  set next-hop 1.1.1.1
  set ipv6 next-hop 3333:2222::
```

show route-map

View the current route map configurations.

S5000

Syntax	`show route-map`
Command Modes	- EXEC - EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
FTOS#show route-map
!
route-map Rmap1, permit, sequence 10
 Match clauses:
  ip address: v4plist
  ipv6 address: plist1
  ipv6 next-hop prefix-lists: plist2
  ipv6 route-source prefix-lists: plist3
```

```
Set clauses:
 next-hop 1.1.1.1
 ipv6 next-hop 3333:2222::
```

Related Commands

route-map – configures a route map.

25

IPv6 Basics

IPv6 Basic Commands are supported on the Dell Networking S5000 switch.

NOTE: For information about the Dell Networking operating software (FTOS) version and platform that supports IPv6 in each software feature, refer to the "IPv6 Addressing" chapter of the *FTOS Configuration Guide*.

clear ipv6 fib

Clear (refresh) all forwarding information base (FIB) entries on a stack-unit.

S5000

Syntax `clear ipv6 fib stack—unit unit-number`

Parameters

unit-number	Enter the keyword `stack-unit` followed by the stack-unit number to clear the FIB for that unit. The range is 0 to 11.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ipv6 route

Clear (refresh) all or a specific route from the IPv6 routing table.

S5000

Syntax `clear ipv6 route {* | ipv6-address prefix-length}`

Parameters

*****	Enter the `*` to clear (refresh) all routes from the IPv6 routing table.
ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

clear ipv6 mld_host

Clear the IPv6 MLD host counters and reset the elapsed time.

S5000

Syntax	`clear ipv6 mld_host`
Command Modes	EXEC
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ipv6 address autoconfig

Configure IPv6 address auto-configuration for the management interface.

S5000

Syntax	`ipv6 address autoconfig` To disable the address autoconfig operation on the management interface, use the `no ipv6 address autoconfig` command.
Default	Disabled
Command Modes	INTERFACE (management interface only)
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ipv6 address

Configure an IPv6 address to an interface.

S5000

Syntax	`ipv6 address {`*`ipv6-address prefix-length`*`}`

To remove the IPv6 address, use the `no ipv6 address {ipv6-address prefix-length}` command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

Defaults none

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information FTOS allows multiple IPv6 addresses to be configured on an interface. When the `no ipv6 address` command is issued without specifying a particular IPv6 address, all IPv6 addresses on that interface are deleted.

Example

```
FTOS(conf)#interface tengigabitethernet 10/0
FTOS(conf-if-te-10/0)#ipv6 address ?
X:X:X:X::X IPv6 address
FTOS(conf-if-te-10/0)#ipv6 address 2002:1:2::3 ?
<0-128> Prefix length in bits
FTOS(conf-if-te-10/0)#ipv6 address 2002:1:2::3 /96 ?
<cr>
FTOS(conf-if-te-10/0)#ipv6 address 2002:1:2::3 /96
FTOS(conf-if-te-10/0)#show config
!
interface TenGigabitEthernet 10/0
  no ip address
  ipv6 address 2002:1:2::3 /96
  no shutdown
FTOS(conf-if-te-10/0)#
```

ipv6 control-plane icmp error-rate-limit

Configure the maximum number of ICMP error packets per second that can be sent per second.

S5000

Syntax `ipv6 control-plane icmp error-rate-limit {1-200}`

To restore the default value, use the `no ipv6 control-plane icmp error-rate-limit` command.

Parameters

pps	Enter the maximum number of error packets to be generated per second. The range is 1 to 200, where 0 disables the rate-limiting.

Default	100 pps
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ipv6 flowlabel-zero

Configure system to set the flow label field in the packets to zero.

S5000

Syntax

```
ipv6 flowlabel-zero
```

To disable the 0 from being set in the field and allow the field to be filled by protocol operations, use the `no ipv6 flowlabel-zero` command.

Default	Disabled
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	If the flowlabel value is already set for BGP or SSH, the system defaults to the already configured value. All packets on the same connection are considered part of the same flow by the system. For new connections, set the new flowlabel to zero.

ipv6 host

Assign a name and IPv6 address to be used by the host-to-IP address mapping table.

S5000

Syntax

```
ipv6 host name ipv6-address
```

Parameters

name	Enter a text string to associate with one IP address.
ipv6-address	Enter the IPv6 address (X:X:X:X::X) to be mapped to the name.

Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ipv6 name-server

Enter up to six IPv6 addresses of name servers. The order you enter the addresses determines the order of their use.

S5000

Syntax

```
ipv6 name-server ipv6-address [ipv6-address2... ipv6-address6]
```

Parameters

ipv6-address	Enter the IPv6 address (X:X:X:X::X) of the name server to be used.
ipv6-address2... ipv6-address6	Enter up five more IP addresses, in dotted decimal format, of name servers to be used. Separate the addresses with a space.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information You can separately configure both IPv4 and IPv6 domain name servers.

ipv6 nd dad attempts

Configure the number of neighbor solicitation messages that are sent to perform duplicate address detection (DAD) on the management interface.

S5000

Syntax

```
ipv6 nd dad attempts {number of attempts}
```

To restore the default value, use the `no ipv6 nd dad attempts` command.

Parameters

number of attempts	Enter the number of attempts to be made to detect a duplicate address The range is 0 to 15. Setting the value to 0 disables DAD on the interface.

Default 3 attempts

Command Modes INTERFACE (management interface only)

Command History

Version 9.0(1.3)	Introduced on the S5000.

ipv6 nd prefix

Specify which IPv6 prefixes are included in Neighbor Advertisements.

S5000

Syntax

```
ipv6 nd prefix {ipv6-prefix | prefix-length | default} [no-
advertise] | [no-autoconfig] [no-rtr-address] [off-link]
[lifetime {valid | infinite} {preferred | infinite}]
```

Parameters

ipv6-prefix	Enter an IPv6 prefix.
prefix-length	Enter the prefix followed by the prefix length. The length range is 0 to 128.
default	Enter the keyword `default` to set default parameters for all prefixes.
no-advertise	Enter the keyword `no-advertise` to prevent the specified prefix from being advertised.
no-autoconfig	Enter the keywords `no-autoconfig` to disable Stateless Address Autoconfiguration.
no-rtr-address	Enter the keyword `no-rtr-address` to exclude the full router address from router advertisements (the R bit is not set).
off-link	Enter the keywords `off-link` to advertise the prefix without stating to recipients that the prefix is either on-link or off-link.
***valid-lifetime* | infinite**	Enter the amount of time that the prefix is advertised, or enter `infinite` for an unlimited amount of time. The range is 0 to 4294967295. The default is **2592000**. The maximum value means that the preferred lifetime does not expire for the valid-life time parameter.
***preferred-lifetime* | infinite**	Enter the amount of time that the prefix is preferred, or enter `infinite` for an unlimited amount of time. The range is 0 to 4294967295. The default is **604800**. The maximum value means that the preferred lifetime does not expire.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

By default, all prefixes configured as addresses on the interface are advertised. This command allows control over the individual parameters per prefix; you can use the `default` keyword to use the default parameters for all prefixes. If a prefix has been configured with lifetime parameter values, the default values cannot be applied using the `ipv6 nd prefix default no-autoconfig` command.

ipv6 route

Establish a static IPv6 route.

S5000

Syntax

`ipv6 route ipv6-address prefix-length {ipv6-address | interface | interface ipv6-address} [distance] [tag value] [permanent]`

To remove the IPv6 route, use the `no ipv6 route ipv6-address prefix-length {ipv6-address | interface | interface ipv6-address} [distance] [tag value] [permanent]` command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information. • For a loopback interface, enter the keyword `loopback` followed by a number from zero (0) to 16383. • For the null interface, enter the keyword `null` followed by zero (0). • For a VLAN interface, enter the keyword `VLAN` followed by the vlan number. • For a port channel interface, enter the keyword `port-channel` followed by the port channel number. If you configure a static IPv6 route using an egress interface and enter the `ping` command to reach the destination IPv6 address, the ping operation may not work. Configure the IPv6 route using a next-hop IPv6 address in order for the `ping` command to detect the destination address.
ipv6-address	(OPTIONAL) Enter the forwarding router IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
distance	(OPTIONAL) Enter a number as the metric distance assigned to the route. The range is 1 to 255.

tag *value*	(OPTIONAL) Enter the keyword `tag` followed by a tag value number. The range is 1 to 4294967295.
permanent	(OPTIONAL) Enter the keyword `permanent` to specify that the route is not to be removed, even if the interface assigned to that route goes down. **NOTE:** If you disable the interface with an IPv6 address associated with the keyword `permanent`, the route disappears from the routing table.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When the interface goes down, FTOS withdraws the route. The route is re-installed, by FTOS, when the interface comes back up. When a recursive resolution is “broken,” FTOS withdraws the route. The route is re-installed, by FTOS, when the recursive resolution is satisfied.

After an IPv6 static route interface is created, if an IP address is not assigned to a peer interface, the peer must be manually pinged to resolve the neighbor information.

Example

```
FTOS(conf)#ipv6 route 44::0 /64 33::1 ?
<1-255>                  Distance metric for this route
permanent                Permanent route
tag                      Set tag for this route

FTOS(conf)#ipv6 route 55::0 /64 ?
X:X:X:X::X               Forwarding router's address
gigabitethernet          Gigabit Ethernet interface
loopback                 Loopback interface
null                     Null interface
port-channel             Port channel interface
tenGigabitethernet       TenGigabit Ethernet interface
vlan                     VLAN interface

FTOS(conf)#ipv6 route 55::0 /64 tengigabitethernet 9/0 ?
<1-255>                  Distance metric for this route
X:X:X:X::X               Forwarding router's address
permanent                Permanent route
tag                      Set tag for this route

FTOS(conf)#ipv6 route 55::0 /64 tengigabitethernet 9/0 66::1 ?
<1-255>                  Distance metric for this route
permanent                Permanent route
tag                      Set tag for this route
FTOS#
```

Related Commands

show ipv6 route – views the IPv6 configured routes.

show ipv6 cam stack-unit

Displays the IPv6 CAM entries for the specified stack-unit.

S5000

Syntax

```
show ipv6 cam stack-unit unit-number port-set {number} [summary
| index | ipv6 address]
```

Parameters

stack-unit ***unit-number***	Enter the keyword `stack unit`' followed by the unit number. The range is 0 to 11.
port-set	Enter the keyword `port pet` followed by the port number. Values are 0 or 1.
summary	(OPTIONAL) Enter the keyword `summary` to display a table listing network prefixes and the total number prefixes which can be entered into the IPv6 CAM.
index	(OPTIONAL) Enter the index in the IPv6 CAM.
ipv6-address	Enter the IPv6 address in the x:x:x:x::x/n format to display networks that have more specific prefixes. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

On the S5000, First-Hop information is not shown for installed routes in the IPv6 content addressable memory (CAM). However, the same is shown in the forwarding information base (FIB).

NOTE: If a route has a mask greater than 64, no output is displayed and no output is displayed for `show ipv6 cam stack-unit unit-number port-set {0-1} ipv6-address`, but an equivalent /64 entry would be listed in the `show ipv6 cam stack-unit unit-number port-set {0-1}` output. Similarly, if there is more than one ECMP object with a destination route that has a mask greater than 64, if the first 64 bits in the destination routes of the ECMP objects are the same, only one route is installed in CAM even though multiple ECMP path entries exist.

NOTE: On the S5000, the self address is displayed in the neighbor portion for the `show ipv6 cam stack-unit unit-number port-set` command.

show ipv6 control-plane icmp

Displays the status of the icmp control-plane setting for the error eate limit setting.

S5000

Syntax	`show ipv6 control-plane icmp`
Default	100
Command Modes	EXEC
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	ipv6 flowlabel-zero – Configure IPv6 address auto-configuration for the management interface.

show ipv6 fib stack-unit

View all FIB entries.

S5000

Syntax

`show ipv6 fib stack-unit unit-number [summary | ipv6-address]`

Parameters

stack-unit *unit-number*	Enter the keyword `stack-unit` followed by the unit number. The range is 0 to 11.
summary	(OPTIONAL) Enter the keyword `summary` to view a summary of entries in IPv6 cam.
ipv6-address	Enter the IPv6 address in the x:x:x:x::x/n format to display networks that have more specific prefixes. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Host tables are not stored in CAM tables on the S5000. Entries for `camIndex` displays as zero (0) on the `show ipv6 fib stack-unit` output for neighbor entries, such as address resolution protocol (ARP) entries.

show ipv6 flowlabel-zero

Display the flow label zero setting.

S5000

Syntax	`show ipv6 flowlabel-zero`	
Default	Disabled	
Command Modes	EXEC	
Command History	**Version 9.0(1.3)**	Introduced on the S5000.
Related Commands	ipv6 nd dad attempts – Configure system to set the flow label field in the packets to zero.	

show ipv6 interface

Display the status of interfaces configured for IPv6.

S5000

Syntax

```
show ipv6 interface type slot/port [brief] [configured] [stack—
unit unit-number]]
```

Parameters

interface *type slot/port*	(OPTIONAL) Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
brief	(OPTIONAL) View a summary of IPv6 interfaces.

configured	(OPTIONAL) View information on all IPv6 configured interfaces.
stack-unit *unit-number*	(OPTIONAL) View information for a specific stack-unit. The range is 0 to 11.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The Management port is enabled by default (`no shutdown`). If necessary, use the `ipv6 address` command to assign an IPv6 address to the Management port.

Example

```
FTOS#
FTOS#show ipv6 int te 0/5
TenGigabitEthernet 0/5 is up, line protocol is up
  IPV6 is enabled
  Link Local address: fe80::201:e8ff:fe8a:e8f7
  Global Unicast address(es):
    2001::1, subnet is 2001::/64
    2002::1, subnet is 2002::/120
    2003::1, subnet is 2003::/120
    2004::1, subnet is 2004::/32
  Global Anycast address(es):
  Joined Group address(es):
    ff02::1
    ff02::2
    ff02::1:ff00:1
    ff02::1:ff8a:e8f7
  ND MTU is 0
  ICMP redirects are not sent
  DAD is enabled, number of DAD attempts: 3
  ND reachable time is 0 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 to 600 seconds
  ND router advertisements live for 1800 seconds

FTOS#
```

Example (Managementethernet)

```
FTOS#
FTOS#show ipv6 int man 0/0
ManagementEthernet 0/0 is up, line protocol is up
  IPV6 is enabled
  Link Local address: fe80::201:e8ff:fe8a:e8f7
  Global Unicast address(es):
    Actual address is 600::1, subnet is 600::/64
     Virtual-IP IPv6 address is not set
  Global Anycast address(es):
  Joined Group address(es):
  IPv6 Basics | 785
    ff02::1
    ff02::1:ff00:1
    ff02::1:ff8a:e8f7
  ND MTU is 1500
  ICMP redirects are not sent
  DAD is enabled, number of DAD attempts: 3
  ND reachable time is 31000 milliseconds
  ND base reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND hop limit is 64

FTOS#
```

Example (Brief)

```
FTOS#show ipv6 interface brief

TenGigabitEthernet 0/0        [up/up]
    fe80::201:e8ff:fe3a:143e
    10::1/64
...
ManagementEthernet 0/0     [up/up]
    fe80::201:e8ff:fe5d:b74c
    fdaa:bbbb:cccc:1004::50/64
...
Vlan 3                     [up/up]
    fe80::201:e8ff:fe3a:19b7
```

show ipv6 mld_host

Display the IPv6 MLD host counters.

S5000

Syntax `show ipv6 mld_host`

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ipv6 mld-host` command shown in the Example below:

Valid MLD Packets	The total number of packets received and sent from the last time the elapsed time was cleared.
Reports	The total number of reports (queries and unsolicited reports generated from joins or leaves) that have been received or sent.
Leaves	The number of Multicast leaves that have been sent.
MLDv1 queries	The number of MLDv1 queries that have been received.
MLDv2 queries	The number of MLDv2 queries that have been received.
Malformed Packets	The number of MLDv1 and MLDv2 packets that do not match the requirement for a valid MLD packet.

Example

```
MLD Host Traffic Counters
Elapsed time since counters cleared: 0028:33:52
                      Received   Sent
Valid MLD Packets  97962      18036
```

```
Reports            79962      18034
Leaves             ----       0
MLDv2 Queries      18000      ----
MLDv1 Queries      0          ----
Errors:
Malformed Packets: 4510
```

show ipv6 route

Displays the IPv6 routes.

S5000

Syntax

`show ipv6 route [`*`ipv6-address prefix-length`*`] [hostname] [all] [bgp `*`as number`*`] [connected] [isis tag] [list `*`prefix-list name`*`] [ospf `*`process-id`*`] [static] [summary]`

Parameters

ipv6-address prefix-length	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
hostname	(OPTIONAL) View information for this IPv6 routes with Host Name.
all	(OPTIONAL) View information for all IPv6 routes.
bgp	(OPTIONAL) View information for all IPv6 BGP routes.
connected	(OPTIONAL) View only the directly connected IPv6 routes.
isis	(OPTIONAL) View information for all IPv6 IS-IS routes.
list	(OPTIONAL) View the IPv6 prefix list.
ospf	(OPTIONAL) View information for all IPv6 OSPF routes.
static	(OPTIONAL) View only routes configured by the `ipv6 route` command.
summary	(OPTIONAL) View a brief list of the configured IPv6 routes.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ipv6 route` command shown in the Examples below.

Field	Description
(undefined)	Identifies the type of route: • L = Local • C = connected • S = static • R = RIP • B = BGP • IN = internal BGP • EX = external BGP • LO = Locally Originated • O = OSPF • IA = OSPF inter area • N1 = OSPF NSSA external type 1 • N2 = OSPF NSSA external type 2 • E1 = OSPF external type 1 • E2 = OSPF external type 2 • i = IS-IS • L1 = IS-IS level-1 • L2 = IS-IS level-2 • IA = IS-IS inter-area • * = candidate default • > = non-active route • + = summary routes
Destination	Identifies the route's destination IPv6 address.
Gateway	Identifies whether the route is directly connected and on which interface the route is configured.
Dist/Metric	Identifies if the route has a specified distance or metric.
Last Change	Identifies when the route was last changed or configured.

Example

```
FTOS#show ipv6 route

Codes:C-connected, L-local, S-static, R-RIP,
 B-BGP, IN-internal BGP, EX-external BGP,LO-Locally Originated,
 O-OSPF, IA-OSPF inter area, N1-OSPF NSSA external type 1,
 N2-OSPF NSSA external type 2, E1-OSPF external type 1,
 E2-OSPF external type 2, i-IS-IS, L1-IS-IS level-1,
 L2-IS-IS level-2, IA- IS-IS inter area, *-candidate default,
Gateway of last resort is not set

   Destination Dist/Metric, Gateway, Last Change
----------------------------------------------
  C  2001::/64 [0/0]
      Direct, Te 1/1, 00:28:49
  C  2002::/120 [0/0]
      Direct, Te 1/1, 00:28:49
  C  2003::/120 [0/0]
      Direct, Te 1/1, 00:28:49
  C  2004::/32 [0/0]
      Direct, Te 1/1, 00:28:49
  L  fe80::/10 [0/0]
      Direct, Nu 0, 00:29:09
```

Example (Summary)

```
FTOS#show ipv6 route summary

Route Source  Active Routes  Non-active Routes
connected     5              0
static        0              0
Total         5              0
Total 5 active route(s) using 952 bytes
```

trust ipv6-diffserv

Allows the dynamic classification of IPv6 DSCP.

S5000

Syntax

```
trust ipv6-diffserv
```

To remove the definition, use the `no trust ipv6-diffserv` command.

Defaults

none

Command Modes

CONFIGURATION-POLICY-MAP-IN

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you configure trust IPv6 diffserv, matched bytes/packets counters are not incremented in the `show qos statistics` command.

Trust diffserv (IPv4) can co-exist with trust ipv6-diffserv in an Input Policy Map. Dynamic classification happens based on the mapping as shown between the IPv6 Serivce Class Field (on left) and the Queue ID (on right)):

IPv6 Service Class Field	Description
111XXXXX — 7	7
110XXXXX — 6	6
101XXXXX — 5	5
100XXXXX — 4	4
011XXXXX — 3	3
010XXXXX — 2	2
001XXXXX — 1	1
000XXXXX — 0	0

26

IPv6 Border Gateway Protocol (IPv6 BGP)

IPv6 Border Gateway Protocol (IPv6 BGP) is supported on the Dell Networking S5000 switch.

This chapter includes the following sections:

- IPv6 BGP Commands
- IPv6 MBGP Commands

IPv6 BGP Commands

BGP is an external gateway protocol that transmits interdomain routing information within and between autonomous systems (AS). BGP version 4 (BGPv4) supports classless interdomain routing and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

The following commands allow you to configure and enable BGP.

aggregate-address

Summarize a range of prefixes to minimize the number of entries in the routing table.

S5000

Syntax

```
aggregate-address ipv6-address prefix-length [advertise-map
map-name] [as-set] [attribute-map map-name] [summary-only]
[suppress-map map-name]
```

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the / x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
advertise-map *map-name*	(OPTIONAL) Enter the keywords `advertise-map` followed by the name of a configured route map to set filters for advertising an aggregate route.
as-set	(OPTIONAL) Enter the keywords `as-set` to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.

attribute-map *map-name*	(OPTIONAL) Enter the keywords `attribute-map` followed by the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
summary-only	(OPTIONAL) Enter the keywords `summary-only` to advertise only the aggregate address. Specific routes are not advertised.
suppress-map *map-name*	(OPTIONAL) Enter the keywords `suppress-map` followed by the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

Defaults	Not configured.
Command Modes	CONFIGURATION-ROUTER-BGPV6-ADDRESS FAMILY
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active. Do not add the `as-set` parameter to the aggregate if routes within the aggregate are constantly changing as the aggregate will flap to keep track of the changes in the AS_PATH. In route maps used in the `suppress-map` parameter, routes meeting the `deny` clause are not suppress; in other words, they are allowed. The opposite is true: routes meeting the `permit` clause are suppressed. If the route is injected using the `network` command, that route still appears in the routing table if you configure the `summary-only` parameter in the `aggregate-address` command. The `summary-only` parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the `neighbor distribute-list` command. In the `show ip bgp ipv6 unicast` command, aggregates contain an ‘a’ in the first column and routes suppressed by the aggregate contain an ‘s’ in the first column.

bgp always-compare-med

Allows you to enable comparison of the MULTI_EXIT_DISC (MED) attributes in the paths from different external ASs.

S5000

Syntax	`bgp always-compare-med` To disable comparison of MED, use the `no bgp always-compare-med` command.
Defaults	Disabled (that is, the software only compares MEDs from neighbors within the same AS).
Command Modes	ROUTER BGP

Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Any update without a MED attribute is the least preferred route. If you enable this command, use the `capture bgp-pdu max-buffer-size *` command to recompute the best path.

bgp bestpath as-path ignore

Ignore the AS PATH in BGP best path calculations.

S5000

Syntax	`bgp bestpath as-path ignore` To return to the default, use the `no bgp bestpath as-path ignore` command.
Defaults	Disabled (that is, the software considers the AS_PATH when choosing a route as best).
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	If you enable this command, use the `capture bgp-pdu max-buffer-size *` command to recompute the best path.

bgp bestpath med confed

Enable MULTI_EXIT_DISC (MED) attribute comparison on paths learned from BGP confederations.

S5000

Syntax	`bgp bestpath med confed` To disable MED comparison on BGP confederation paths, use the `no bgp bestpath med confed` command.
Defaults	Disabled.
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	The software compares the MEDs only if the path contains no external autonomous system numbers.

If you enable this command, use the `capture bgp-pdu max-buffer-size *` command to recompute the best path.

bgp bestpath med missing-as-best

During path selection, indicate a preference to paths with missing MED (MULTI_EXIT_DISC) over those paths with an advertised MED attribute.

S5000

Syntax

`bgp bestpath med missing-as-best`

To return to the default selection, use the `no bgp bestpath med missing-as-best` command.

Defaults

Disabled.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The MED is a 4-byte unsigned integer value and the default behavior is to assume a missing MED as 4294967295. This command causes a missing MED to be treated as 0. During path selection, paths with a lower MED are preferred over those with a higher MED.

bgp client-to-client reflection

Allows you to enable route reflection between clients in a cluster.

S5000

Syntax

`bgp client-to-client reflection`

To disable client-to-client reflection, use the `no bgp client-to-client reflection` command.

Defaults

Enabled when a route reflector is configured.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Route reflection to clients is not necessary if all client routers are fully meshed.

Related Commands

bgp cluster-id – assigns and ID to a BGP cluster with two or more route reflectors.

neighbor route-reflector-client – configures a route reflector and clients.

bgp cluster-id

Assign a cluster ID to a BGP cluster with more than one route reflector.

S5000

Syntax

`bgp cluster-id {ip-address | number}`

To delete a cluster ID, use the `no bgp cluster-id {ip-address | number}` command.

Parameters

ip-address	Enter an IP address as the route reflector cluster ID.
number	Enter a route reflector cluster ID as a number from 1 to 4294967295.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When a BGP cluster contains only one route reflector, the cluster ID is the route reflector's router ID. For redundancy, a BGP cluster may contain two or more route reflectors and you assign a cluster ID with the `bgp cluster-id` command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster.

The default format for displaying the cluster-id is dotted decimal, but if you enter the cluster-id as an integer, it is displayed as an integer.

Related Commands

bgp client-to-client reflection – enables route reflection between the route reflector and the clients.

neighbor route-reflector-client – configures a route reflector and clients.

show ip bgp ipv6 unicast cluster-list – views paths with a cluster ID.

bgp confederation identifier

Configure an identifier for a BGP confederation.

S5000

Syntax

`bgp confederation identifier as-number`

To delete a BGP confederation identifier, use the `no bgp confederation identifier as-number` command.

Parameters

as-number	Enter the AS number. The range is 1 to 65535.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation.

FTOS accepts confederation EBGP peers without a LOCAL_PREF attribute. The software sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.

bgp confederation peers

Specify the autonomous systems (ASs) that belong to the BGP confederation.

S5000

Syntax

```
bgp confederation peers as-number [...as-number]
```

To remove bgp confederation peers, use the `no bgp confederation peer` command.

Parameters

as-number	Enter the AS number. The range is 1 to 65535.
...as-number	(OPTIONAL) Enter up to 16 confederation numbers. The range is 1 to 65535.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The Autonomous Systems configured in this command are visible to the EBGP neighbors. Each Autonomous System is fully meshed and contains a few connections to other Autonomous Systems.

After specifying autonomous systems numbers for the BGP confederation, recycle the peers to update their configuration.

Related Commands

bgp confederation identifier – configures a confederation ID.

bgp dampening

Enable BGP route dampening and configure the dampening parameters.

S5000

Syntax

```
bgp dampening [half-life reuse suppress max-suppress-time]
[route-map map-name]
```

Parameters

half-life	(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half, after the half-life period expires. The range is 1 to 45. The default is **15 minutes**.
reuse	(OPTIONAL) Enter a number as the reuse value, which is compared to the flapping route's Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed). The range is 1 to 20000. The default is **750**.
suppress	(OPTIONAL) Enter a number as the suppress value, which is compared to the flapping route's Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed). The range is 1 to 20000. The default is **2000**.
max-suppress-time	(OPTIONAL) Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value. The range is 1 to 255. The default is **60 minutes**.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of a configured route map. Only match commands in the configured route map are supported.

Defaults

Disabled.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you enter `bgp dampening`, the default values for `half-life`, `reuse`, `suppress`, and `max-suppress-time` are applied. The parameters are position-dependent; therefore, if you configure one parameter, you must configure the parameters in the order they appear in the command.

Related Commands

show ip bgp ipv6 unicast dampened-paths – views the BGP paths.

bgp default local-preference

Change the default local preference value for routes exchanged between internal BGP peers.

S5000

Syntax `bgp default local-preference value`

To return to the default value, use the `no bgp default local-preference` command.

Parameters

value	Enter a number to assign to routes as the degree of preference for those routes. When routes are compared, the higher the degree of preference or local preference value, the more the route is preferred. The range is 0 to 4294967295. The default is **100**.

Defaults **100**

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

bgp enforce-first-as

Disable (or enable) enforce-first-as check for updates received from EBGP peers.

S5000

Syntax `bgp enforce-first-as`

To turn off the default, use the `no bgp enforce-first-as` command.

Defaults Enabled.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This is enabled by default; that is, for all updates received from EBGP peers, BGP ensures that the first AS of the first AS segment is always the AS of the peer. If not, the update is dropped and a counter is incremented. Use the `show ip bgp ipv6 unicast neighbors` command to view the failed enforce-first-as check counter.

If you disable `enforce-first-as`, it can be viewed using the `show ip protocols` command.

Related Commands

show ip bgp ipv6 unicast neighbors – displays IPv6 routing information exchanged by BGP neighbors.

show ip protocols – views information on routing protocols.

bgp fast-external-failover

Enable the fast external failover feature, which immediately resets the BGP session if a link to a directly connected external peer fails.

S5000

Syntax	`bgp fast-external-failover` To disable fast external failover, use the `no bgp fast-external-failover` command.
Defaults	Enabled
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	The `bgp fast-external-failover` command appears in the `show config` command output.

bgp four-octet-as-support

Enable 4-byte support for the BGP process.

S5000

Syntax	`bgp four-octet-as-support` To disable fast external failover, use the `no bgp four-octet-as-support` command.
Defaults	Disabled (supports 2-Byte format)
Command Modes	ROUTER BGP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Routers supporting 4-Byte ASNs advertise that function in the OPEN message. The behavior of a 4-Byte router is slightly different depending on whether it is speaking to a 2-Byte router or a 4-Byte router. When creating Confederations, all the routers in the Confederation must be 4 or 2 byte identified routers. You cannot mix them. Where the 2-Byte format is 1-65535, the 4-Byte format is 1-4294967295. Both formats are accepted, and the advertisements reflect the entered format.

For more information about using the 2- or 4-Byte format, refer to the *FTOS Configuration Guide*.

bgp graceful-restart

Enable graceful restart on a BGP neighbor, a BGP node, or designate a local router to support graceful restart as a receiver only.

S5000

Syntax

```
bgp graceful-restart [restart-time seconds] [stale-path-time
seconds] [role receiver-only]
```

To return to the default, enter the `no bgp graceful-restart` command.

Parameters

neighbor ***ip-address | peer-group-name***	Enter the keyword `neighbor` followed by one of the options listed below: • *`ip-address`* of the neighbor in IP address format of the neighbor • *`peer-group-name`* of the neighbor peer group
restart-time ***seconds***	Enter the keywords `restart-time` followed by the maximum number of seconds needed to restart and bring up all peers. The range is 1 to 3600 seconds. The default is **120 seconds**.
stale-path-time ***seconds***	Enter the keywords `stale-path-time` followed by the maximum number of seconds to wait before restarting a peer's stale paths. The default is **360 seconds**.
role ***receiver-only***	Enter the keywords `role receiver-only` to designate the local router to support graceful restart as a receiver only.

Defaults As above

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This feature is advertised to BGP neighbors through a capability advertisement. In Receiver only mode, BGP saves the advertised routes of peers that support this capability when they restart.

bgp log-neighbor-changes

Enable logging of BGP neighbor resets.

S5000

Syntax

`bgp log-neighbor-changes`

To disable logging, use the `no bgp log-neighbor-changes` command.

Defaults

Enabled.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `bgp log-neighbor-changes` command appears in the `show config` command output.

Related Commands

show config – views the current configuration.

bgp non-deterministic-med

Compare MEDs of paths from different autonomous systems (ASs).

S5000

Syntax

`bgp non-deterministic-med`

To return to the default, use the `no bgp non-deterministic-med` command.

Defaults

Disabled (that is, paths/routes for the same destination but from different ASs does not have their MEDs compared).

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

In non-deterministic mode, paths are compared in the order in which they arrive. This method can lead to FTOS choosing different best paths from a set of paths, depending on the order in which they are received from the neighbors because MED may or may not get compared between adjacent paths. In deterministic mode (`no bgp non-deterministic-med`), FTOS compares MED between adjacent paths within an AS group because all paths in the AS group are from the same AS.

When you change the path selection from deterministic to non-deterministic, the path selection for existing paths remains deterministic until you enter the `capture bgp-pdu max-buffer-size` command to clear existing paths.

bgp recursive-bgp-next-hop

Enable next-hop resolution through other routes learned by BGP.

S5000

Syntax

`bgp recursive-bgp-next-hop`

To disable next-hop resolution, use the `no bgp recursive-bgp-next-hop` command.

Defaults

Enabled.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command is a knob to disable BGP next-hop resolution using BGP learned routes. During the next-hop resolution, only the first route that the next-hop resolves through is verified for the route's protocol source and is checked if the route is learned from BGP or not.

The `clear ip bgp` command is required for this command to take effect and to keep the BGP database consistent. Execute the `clear ip bgp` command right after executing this command.

Related Commands

capture bgp-pdu max-buffer-size

bgp regex-eval-optz-disable

Disables the Regex Performance engine that optimizes complex regular expression with BGP.

S5000

Syntax

`bgp regex-eval-optz-disable`

To re-enable optimization engine, use the `no bgp regex-eval-optz-disable` command.

Defaults

Enabled.

Command Modes

ROUTER BGP (conf-router_bgp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

BGP uses regular expressions (regex) to filter route information. In particular, the use of regular expressions to filter routes based on AS-PATHs and communities is quite common. In a large scale configuration, filtering millions of routes based on regular expressions can be quite CPU intensive, as a regular expression evaluation involves generation and evaluation of complex finite state machines.

BGP policies, containing regular expressions to match as-path and communities, tend to use a lot of CPU processing time, which in turn affects the BGP routing convergence. Additionally, the `show bgp` commands, which are filtered through regular expressions, use up CPU cycles particularly with large databases. The Regex Engine Performance Enhancement feature optimizes the CPU usage by caching and reusing regular expression evaluation results. This caching and reuse may be at the expense of processor memory.

Example

```
FTOS(conf-router_bgp)#no bgp regex-eval-optz-disable
FTOS(conf-router_bgp)#do show ip protocols
Routing Protocol is "ospf 22222"
  Router ID is 2.2.2.2
  Area              Routing for Networks
  51                10.10.10.0/00

Routing Protocol is "bgp 1"
  Cluster Id is set to 10.10.10.0
  Router Id is set to 10.10.10.0
  Fast-external-fallover enabled
Regular expression evaluation optimization enabled
  Capable of ROUTE_REFRESH
  For Address Family IPv4 Unicast
    BGP table version is 0, main routing table version 0
    Distance: external 20 internal 200 local 200
```

bgp router-id

Assign a user-given ID to a BGP router.

S5000

Syntax

`bgp router-id ip-address`

To delete a user-assigned IP address, use the `no bgp router-id` command.

Parameters

ip-address	Enter an IP address in dotted decimal format to reset only that BGP neighbor.

Defaults

The router ID is the highest IP address of the Loopback interface or, if no Loopback interfaces are configured, the highest IP address of a physical interface on the router.

Command Modes

ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Peering sessions are reset when you change the router ID of a BGP router.

bgp soft-reconfig-backup

Use this command *only* when route-refresh is *not* negotiated between peers to avoid having a peer re-send BGP updates.

S5000

Syntax	`bgp soft-reconfig-backup` To return to the default setting, use the `no bgp soft-reconfig-backup` command.
Defaults	Off
Command Modes	ROUTER BGPV6 ADDRESS FAMILY (conf-router_bgpv6_af)
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	When you enable soft-reconfiguration for a neighbor and the `clear ip bgp soft in` is executed, the update database stored in the router is replayed and updates are reevaluated. With this command, the replay and update process is triggered only if route-refresh request is *not* negotiated with the peer. If the request is indeed negotiated (after execution of `clear ip bgp soft in`), BGP sends a route-refresh request to the neighbor and receives all of the peer's updates.
Related Commands	clear ip bgp ipv6 unicast soft – activates inbound policies for IPv6 routes without resetting the BGP TCP session.

capture bgp-pdu max-buffer-size

Set the size of the BGP packet capture buffer. This buffer size pertains to both IPv4 and IPv6 addresses.

S5000

Syntax	`capture bgp-pdu max-buffer-size` *`100-102400000`*
Parameters	***100-102400000*** Enter a size for the capture buffer.
Defaults	40960000 bytes
Command Modes	• EXEC • EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	capture bgp-pdu neighbor (ipv6) – enables route reflection between the route reflector and the clients.

show capture bgp-pdu neighbor – configures a route reflector and clients.

capture bgp-pdu neighbor (ipv6)

Enable capture of an IPv6 BGP neighbor packet.

S5000

Syntax

`capture bgp-pdu neighbor ipv6-address direction {both | rx | tx}`

To disable capture of the IPv6 BGP neighbor packet, use the `no capture bgp-pdu neighbor ipv6-address` command.

Parameters

ipv6-address	Enter the IPv6 address of the target BGP neighbor.
direction {both | rx | tx}	Enter the keyword `direction` and a direction— either `rx` for inbound, `tx` for outbound, or both.

Defaults

Not configured.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

capture bgp-pdu max-buffer-size – enables route reflection between the route reflector and the clients.

show capture bgp-pdu neighbor – configures a route reflector and clients.

capture bgp-pdu neighbor – enables capture of an IPv4 BGP neighbor packet.

clear ip bgp * (asterisk)

Reset all BGP sessions in the specified category on the S5000. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

S5000

Syntax

`clear ip bgp * [ipv4 multicast soft [in | out] | ipv6 unicast soft [in | out] | soft [in | out]]`

Parameters

*****	Enter an asterisk (`*`) to reset all BGP sessions.

ipv4 multicast soft [in | out]	(OPTIONAL) Enter the keywords `ipv4 multicast soft [in	out]` to set options within the specified IPv4 address family.
ipv6 unicast soft [in | out]	(OPTIONAL) Enter the keywords `ipv6 multicast soft [in	out]` to set options within the specified IPv6 address family.
soft	(OPTIONAL) Enter the keyword `soft` to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration. **NOTE:** If you enter `clear ip bgp ip6-address soft`, both inbound and outbound policies are reset.
in	(OPTIONAL) Enter the keyword `in` to activate only inbound policies.
out	(OPTIONAL) Enter the keyword `out` to activate only outbound policies.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ip bgp as-number

Reset BGP sessions on the S5000. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

S5000

Syntax

```
clear ip bgp as-number [flap-statistics | ipv4 {multicast
{flap-statistics | soft {in | out}} | unicast {flap-statistics
| soft {in | out}} | ipv6 unicast {flap-statistics | soft {in |
out}| soft [in | out]
```

Parameters

as-number	Enter an autonomous system (AS) number to reset neighbors belonging to that AS. If used without a qualifier, the keyword resets all neighbors belonging to that AS. The range is 0 to 65535 (2-byte), 1 to 4294967295 (4-byte), or 0.1 to 65535.65535 (dotted format).
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to clear all flap statistics belonging to that AS or a specified address family within that AS.
ipv4	(OPTIONAL) Enter the keyword `ipv4` to select options for that address family.
ipv6	(OPTIONAL) Enter the keyword `ipv6` to select options for that address family.
unicast	(OPTIONAL) Enter the keyword `unicast` to select the unicast option within the selected address family.

multicast	(OPTIONAL) Enter the keyword `multicast` to select the multicast option within the selected address family. Multicast is supported on IPv4 only.
soft	(OPTIONAL) Enter the keyword `soft` to configure and activate policies without resetting the BGP TCP session; that is, BGP Soft Reconfiguration. **NOTE:** If you enter `clear ip bgp ipv6-address soft`, both inbound and outbound policies are reset.
in	(OPTIONAL) Enter the keyword `in` to activate only inbound policies.
out	(OPTIONAL) Enter the keyword `out` to activate only outbound policies.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ip bgp ipv6-address

Reset BGP sessions specific to an IPv6 address on the S5000. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

S5000

Syntax

```
clear ip bgp ipv6-address [flap-statistics | ipv4 {multicast
{flap-statistics | soft {in | out}} | unicast {flap-statistics
| soft {in | out}} | ipv6 unicast {flap-statistics | soft {in |
out}| soft [in | out]
```

Parameters

ipv6-address	Enter an IPv6 address to reset neighbors belonging to that IP. Used without a qualifier, the keyword `ipv6-address` resets all neighbors belonging to that IP.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to clear all flap statistics belonging to that AS or a specified address family within that IP.
ipv4	(OPTIONAL) Enter the keyword `ipv4` to select options for that address family.
ipv6	(OPTIONAL) Enter the keyword `ipv6` to select options for that address family.
unicast	(OPTIONAL) Enter the keyword `unicast` to select the unicast option within the selected address family.

multicast	(OPTIONAL) Enter the keyword `multicast` to select the multicast option within the selected address family. Multicast is supported on IPv4 only.
soft	(OPTIONAL) Enter the keyword `soft` to configure and activate policies without resetting the BGP TCP session; that is, BGP Soft Reconfiguration. **NOTE:** If you enter `clear ip bgp ip6-address soft`, both inbound and outbound policies are reset.
in	(OPTIONAL) Enter the keyword `in` to activate only inbound policies.
out	(OPTIONAL) Enter the keyword `out` to activate only outbound policies.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ip bgp peer-group

Reset a peer-group’s BGP sessions.

S5000

Syntax `clear ip bgp peer-group peer-group-name`

Parameters

peer-group *peer-group-name*	Enter the keyword `peer-group` followed by the peer group name to reset the BGP sessions within that peer group.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ip bgp ipv6 dampening

Clear information on route dampening and return suppressed route to active state.

S5000

Syntax `clear ip bgp ipv6 unicast dampening [ipv6-address]`

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information After you enter this command, the software deletes the history routes and returns the suppressed routes to the active state.

clear ip bgp ipv6 flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

S5000

Syntax

```
clear ip bgp ipv6 unicast flap-statistics [ipv6-address |
filter-list as-path-name | regexp regular-expression]
```

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
filter-list *as-path-name*	(OPTIONAL) Enter the keywords `filter-list` followed by the name of a configured AS-PATH list.
regexp *regular-expression*	(OPTIONAL) Enter the keyword `regexp` followed by regular expressions. Use one or a combination of the following: • . (period) matches on any single character, including white space • * (asterisk) matches on sequences in a pattern (zero or more sequences) • + (plus sign) matches on sequences in a pattern (one or more sequences) • ? (question mark) matches sequences in a pattern (0 or 1 sequences) • [ ] (brackets) matches a range of single-character patterns. • ^ (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.) • $ (dollar sign) matches the end of the output string.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If you enter the `clear ip bgp ipv6 flap-statistics` command without any parameters, all statistics are cleared.

Related Commands show ip bgp ipv6 unicast flap-statistics – views BGP flap statistics.

clear ip bgp ipv6 unicast soft

Clear and reapply policies for IPv6 unicast routes without resetting the TCP connection; that is, perform BGP soft reconfiguration.

S5000

Syntax

```
clear ip bgp {* | as-number | ipv4-neighbor-addr | ipv6-
neighbor-addr | peer-group name} ipv6 unicast soft [in | out]
```

Parameters

*	Clear and reapply policies for all BGP sessions.
as-number	Clear and reapply policies for all neighbors belonging to the AS. The range is 0 to 65535 (2-Byte) 1 to 4294967295 (4-Byte) or 0.1 to . 65535.65535 (Dotted format).
ipv4-neighbor-addr | *ipv6-neighbor-addr*	Clear and reapply policies for a neighbor.
peer-group *name*	Clear and reapply policies for all BGP routers in the specified peer group.
ipv6 unicast	Clear and reapply policies for all IPv6 unicast routes.
in	Reapply only inbound policies. **NOTE:** If you enter `soft`, without an `in` or `out` option, both inbound and outbound policies are reset.
out	Reapply only outbound policies. **NOTE:** If you enter `soft`, without an `in` or `out` option, both inbound and outbound policies are reset.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug ip bgp

Allows you to view all information on BGP, including BGP events, keepalives, notifications, and updates.

S5000

Syntax

```
debug ip bgp [ipv6-address | peer-group peer-group-name] [in |
out]
```

To disable all BGP debugging, use the `no debug ip bgp` command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group *peer-group-name*	Enter the keywords `peer-group` followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view only information on inbound BGP routes.
out	(OPTIONAL) Enter the keyword `out` to view only information on outbound BGP routes.

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To view information on both incoming and outgoing routes, do not include the `in` and `out` parameters in the `debugging` command. The `in` and `out` parameters cancel each other; for example, if you enter `debug ip bgp in` and then enter `debug ip bgp out`, you will not see information on the incoming routes.

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

Related Commands

debug ip bgp events – views information about BGP events.

debug ip bgp keepalives – views information about BGP keepalives.

debug ip bgp notifications – views information about BGP notifications.

debug ip bgp updates – views information about BGP updates.

debug ip bgp events

Allows you to view information on local BGP state changes and other BGP events.

S5000

Syntax

`debug ip bgp [`*`ipv6-address`*` | peer-group `*`peer-group-name`*`] events [in | out]`

To disable debugging, use the `no debug ip bgp `*`ipv6-address`*` | peer-group `*`peer-group-name`*`] events` command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group *peer-group-name*	Enter the keywords `peer-group` followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view only information on inbound BGP routes.
out	(OPTIONAL) Enter the keyword `out` to view only information on outbound BGP routes.

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

debug ip bgp ipv6 dampening

View information on dampened (non-active) IPv6 routes.

S5000

Syntax

`debug ip bgp ipv6 unicast dampening [in | out]`

To disable debugging, use the `no debug ip bgp ipv6 unicast dampening` command.

Parameters

in	(OPTIONAL) Enter the keyword `in` to view only inbound dampened routes.
out	(OPTIONAL) Enter the keyword `out` to view only outbound dampened routes.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

Related Commands show ip bgp ipv6 unicast dampened-paths – views BGP dampened routes.

debug ip bgp ipv6 unicast soft-reconfiguration

Enable soft-reconfiguration debugging for IPv6 unicast routes.

S5000

Syntax `debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv6 unicast soft-reconfiguration`

To disable debugging, use the `no debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv6 unicast soft-reconfiguration` command.

Parameters

ipv4-address | *ipv6-address*	Enter the IP address of the neighbor on which you want to enable soft-reconfiguration debugging.
peer-group-name	Enter the name of the peer group on which you want to enable soft-reconfiguration debugging.
ipv6 unicast	Debug soft reconfiguration for IPv6 unicast routes.

Defaults Disabled.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This command turns on BGP soft-reconfiguration inbound debugging for IPv6 unicast routes. If no neighbor is specified, debug is turned on for all neighbors.

Related Commands show ip bgp ipv6 unicast dampened-paths – views BGP dampened routes.

debug ip bgp keepalives

Allows you to view information about BGP keepalive messages.

S5000

Syntax

```
debug ip bgp [ipv6-address | peer-group peer-group-name]
keepalives [in | out]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] keepalives [in | out]` command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group *peer-group-name*	(OPTIONAL) Enter the keywords `peer-group` followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view only inbound keepalive messages.
out	(OPTIONAL) Enter the keyword `out` to view only outbound keepalive messages.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

debug ip bgp notifications

Allows you to view information about BGP notifications received from neighbors.

S5000

Syntax

```
debug ip bgp [ipv6-address | peer-group peer-group-name]
notifications [in | out]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] notifications [in | out]` command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

peer-group *peer-group-name*	(OPTIONAL) Enter the keywords `peer-group` followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view BGP notifications received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view BGP notifications sent to neighbors.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

debug ip bgp updates

Allows you to view information about BGP updates.

S5000

Syntax

```
debug ip bgp [ipv6-address | peer-group peer-group-name | ipv6
unicast [ipv6-address]] updates [in | out | prefix-list prefix-
list-name]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name | ipv6 unicast [ipv6-address]] updates [in | out]` command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group *peer-group-name*	(OPTIONAL) Enter the keywords `peer-group` followed by the name of the peer group.
ipv6 unicast [*ipv6-address*]	(OPTIONAL) Enter the keywords `ipv6 unicast`, and, optionally, an ipv6 address.
in	(OPTIONAL) Enter the keyword `in` to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view only BGP updates sent to neighbors.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

default-metric

Allows you to change the metrics of redistributed routes to locally originated routes. Use this command with the `redistribute` command.

S5000

Syntax `default-metric` *`number`*

To return to the default setting, use the `no default-metric` command.

Parameters

number	Enter a number as the metric to be assigned to routes from other protocols. The range is 1 to 4294967295.

Defaults 0

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The `default-metric` command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.

Related Commands

bgp always-compare-med – enables comparison of all BGP MED attributes.

redistribute – redistributes routes from other routing protocols into BGP.

description

Enter a description of the BGP routing protocol.

S5000

Syntax `description {`*`description`*`}`

To remove the description, use the no description {*description*} command.

Parameters

description	Enter a description to identify the BGP protocol (80 characters maximum).

Defaults none

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

router bgp – enters ROUTER mode on the switch.

distance bgp

Configure three administrative distances for routes.

S5000

Syntax

`distance bgp external-distance internal-distance local-distance`

To return to default values, use the `no distance bgp` command.

Parameters

external-distance	Enter a number to assign to routes learned from a neighbor external to the AS. The range is 1 to 255. The default is **20**.
internal-distance	Enter a number to assign to routes learned from a router within the AS. The range is 1 to 255. The default is **200**.
local-distance	Enter a number to assign to routes learned from networks listed in the network command. The range is 1 to 255. The default is **200**.

Defaults

- external-distance = **20**
- internal-distance = **200**
- local-distance = **200**

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

△ **CAUTION: Dell Networking recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.**

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table.

Routes from confederations are treated as internal BGP routes.

maximum-paths

Configure the maximum number of parallel routes (multipath support) BGP supports.

S5000

Syntax `maximum-paths {ebgp | ibgp} number`

To return to the default values, use the `no maximum-paths` command.

Parameters

ebgp	Enter the keyword `ebgp` to enable multipath support for External BGP routes.
ibgp	Enter the keyword `ibgp` to enable multipath support for Internal BGP routes.
number	Enter a number as the maximum number of parallel paths. The range is 1 to 16. The default is **1**.

Defaults 1

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If you enable this command, use the `capture bgp-pdu max-buffer-size` command to recompute the best path.

neighbor activate

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI.

S5000

Syntax `neighbor {ipv6-address | peer-group-name} activate`

To disable, use the `no neighbor {ipv6-address | peer-group-name} activate` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Identify a peer group by name.
activate	Enter the keyword `activate` to enable the identified neighbor or peer group in the new AFI/SAFI.

Defaults	Disabled.
Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	By default, when a neighbor/peer group configuration is created in the Router BGP context, it is enabled for the IPv6/Unicast AFI/SAFI. By using `activate` in the new context, the neighbor/peer group is enabled for AFI/SAFI.

neighbor advertisement-interval

Set the advertisement interval between BGP neighbors or within a BGP peer group.

S5000

Syntax

`neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} advertisement-interval `*`seconds`*

To return to the default value, use the `no neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} advertisement-interval` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
seconds	Enter a number as the time interval, in seconds, between BGP advertisements. The range is 0 to 600 seconds. The default is **5 seconds** for internal BGP peers and **30 seconds** for external BGP peers.

Defaults

- seconds = **5 seconds** (internal peers)
- seconds = **30 seconds** (external peers)

Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	**Version 9.0(1.3)** Introduced on the S5000.

neighbor allowas-in

Set the number of times an AS number can occur in the AS path.

S5000

Syntax

`neighbor {ip-address | peer-group-name} allowas-in number`

To return to the default value, use the `no neighbor {ip-address | peer-group-name} allowas-in` command.

Parameters

ip-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
number	Enter a number of times to allow this neighbor ID to use the AS path. The range is 1 to 10.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

bgp four-octet-as-support – enables 4-Byte support for the BGP process.

neighbor default-originate

Inject the default route to a BGP peer or neighbor.

S5000

Syntax

`neighbor {ipv6-address | peer-group-name} default-originate [route-map map-name]`

To remove a default route, use the `no neighbor {ipv6-address | peer-group-name} default-originate [route-map map-name]` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the default route of all routers in that peer group.

route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If you apply a route map to a BGP peer or neighbor with the `neighbor default-originate` command configured, the software does not apply the set filters in the route map to that BGP peer or neighbor.

neighbor description

Assign a character string describing the neighbor or group of neighbors (peer group).

S5000

Syntax

```
neighbor {ipv6-address | peer-group-name} description text
```

To delete a description, use the `no neighbor {ipv6-address | peer-group-name} description text` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
text	Enter a continuous text string up to 80 characters.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

neighbor distribute-list

Distribute BGP information using an established prefix list.

S5000

Syntax

`neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}`

To delete a neighbor distribution list, use the `no neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
prefix-list-name	Enter the name of an established prefix list. If the prefix list is not configured, the default is **permit** (to allow all routes).
in	Enter the keyword in to distribute only inbound traffic.
out	Enter the keyword out to distribute only outbound traffic.

Defaults

Not configured.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

neighbor filter-list – assigns a AS-PATH list to a neighbor or peer group.

neighbor route-map – assigns a route map to a neighbor or peer group.

neighbor ebgp-multihop

Attempt and accept BGP connections to external peers on networks that are not directly connected.

S5000

Syntax

`neighbor {ipv6-address | peer-group-name} ebgp-multihop [ttl]`

To disallow and disconnect connections, use the `no neighbor {ipv6-address | peer-group-name} ebgp-multihop [ttl]` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

peer-group-name	Enter the name of the peer group.
ttl	(OPTIONAL) Enter the number of hops as the time to live (ttl) value. The range is 1 to 255. The default is **255**.

Defaults Disabled.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information To prevent loops, the `neighbor ebgp-multihop` command does not install default routes of the multihop peer. Networks not directly connected are not considered valid for best path selection.

neighbor fall-over

Enable or disable fast fall-over for BGP neighbors.

S5000

Syntax `neighbor {ipv6-address | peer-group-name} fall-over`

To disable, use the `no neighbor {ipv6-address | peer-group-name} fall-over` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.

Defaults Disabled.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000

Usage Information When you enable fall-over, BGP keeps track of IP or IPv6 reachability to the peer remote address and the peer local address. Whenever either address becomes unreachable (for examle, no active route exists in the routing table for peer IP or IPv6 destination/local address), BGP brings down the session with the peer.

Related Commands show ip bgp ipv6 unicast neighbors – displays IPv6 routing information exchanged by BGP neighbors.

neighbor filter-list

Configure a BGP filter based on the AS-PATH attribute.

S5000

Syntax	`neighbor {`*`ipv6-address`*`	`*`peer-group-name`*`} filter-list `*`as-path-name`*` {in	out}` To delete a BGP filter, use the `no neighbor {`*`ipv6-address`*`	`*`peer-group-name`*`} filter-list `*`as-path-name`*` {in	out}` command.
Parameters	

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to apply the filter to all routers in the peer group.
in	Enter the keyword `in` to filter inbound BGP routes.
out	Enter the keyword `out` to filter outbound BGP routes.

Defaults	Not configured.
Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	

Version 9.0(1.3)	Introduced on the S5000.

neighbor maximum-prefix

Control the number of network prefixes received.

S5000

Syntax	`neighbor {`*`ipv6-address`*`	`*`peer-group-name`*`} maximum-prefix `*`maximum`*` [`*`threshold`*`] [warning-only]` To return to the default values, use the `no neighbor {`*`ipv6-address`*`	`*`peer-group-name`*`} maximum-prefix `*`maximum`*` [`*`threshold`*`] [warning-only]` command.
Parameters	

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.

maximum	Enter a number as the maximum number of prefixes allowed for this BGP router. The range is 1 to 4294967295.
threshold	(OPTIONAL) Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches this threshold, the switch software sends a message. The range is 1 to 100 percent. The default is **75**.
warning-only	(OPTIONAL) Enter the keyword `warning-only` to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

Defaults threshold = **75**

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If the `neighbor maximum-prefix` command is configured and the neighbor receives more prefixes than allowed by the `neighbor maximum-prefix` command configuration, the neighbor goes down and the `show ip bgp ipv6 unicast summary` command displays (`prfxd`) in the State/PfxRcd column for that neighbor. The neighbor remains down until you enter the `capture bgp-pdu max-buffer-size` command for the neighbor or the peer group to which the neighbor belongs or you enter `neighbor shutdown` and `neighbor no shutdown` commands.

Related Commands

show ip bgp ipv6 unicast summary – displays the current BGP configuration.

neighbor next-hop-self

Allows you to configure the router as the next hop for a BGP neighbor. (This command is used for IBGP).

S5000

Syntax

`neighbor {ipv6-address | peer-group-name} next-hop-self`

To return to the default setting, use the `no neighbor {ipv6-address | peer-group-name} next-hop-self` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	(OPTIONAL) Enter the name of the peer group.

Defaults Disabled.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If you configure the `set ipv6 next-hop` command in ROUTE-MAP mode, its configuration takes precedence over the `neighbor next-hop-self` command.

neighbor peer-group (assigning peers)

Allows you to assign one peer to a existing peer group.

S5000

Syntax `neighbor` *`ipv6-address`* `peer-group` *`peer-group-name`*

To delete a peer from a peer group, use the `no neighbor` *`ipv6-address`* `peer-group` *`peer-group-name`* command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group *peer-group-name*	Enter the keywords `peer-group` followed by the name of a configured peer group (maximum 16 characters).

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information You can assign up to 64 peers to one peer group.

When you add a peer to a peer group, it inherits all the peer group's configured parameters. A peer cannot become part of a peer group if any of the following commands are configured on the peer:

- neighbor advertisement-intervall
- neighbor distribute-list
- neighbor filter-list
- neighbor next-hop-self
- neighbor route-map
- neighbor route-reflector-client
- neighbor send-community

A neighbor may keep its configuration after it was added to a peer group if the neighbor's configuration is more specific than the peer group's and the neighbor's configuration does not affect outgoing updates.

A peer group must exist before you add a peer to it. If the peer group is disabled (`shutdown`) the peers within the group are also disabled (`shutdown`).

Related Commands	capture bgp-pdu max-buffer-size – resets BGP sessions. neighbor peer-group (creating group) – creates a peer group. show ip bgp ipv6 unicast peer-group – views BGP peers. show ip bgp ipv6 unicast neighbors – views BGP neighbors configurations.

neighbor peer-group (creating group)

Allows you to create a peer group and assign it a name.

S5000

Syntax

```
neighbor peer-group-name peer-group
```

To delete a peer group, use the `no neighbor peer-group-name peer-group` command.

Parameters

peer-group-name	Enter a text string up to 16 characters long as the name of the peer group.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information When a peer group is created, it is disabled (`shut mode`).

Related Commands	neighbor peer-group (assigning peers) – assigns routers to a peer group. neighbor remote-as – assigns a indirectly connected AS to a neighbor or peer group. neighbor shutdown – disables a peer or peer group.

neighbor peer-group passive

Enable passive peering on a BGP peer group; that is, the peer group does not send an OPEN message, but does respond to one.

S5000

Syntax

```
neighbor peer-group-name peer-group passive
```

To delete a passive peer-group, use the `no neighbor` *`peer-group-name`* `peer-group passive` command.

Parameters

peer-group-name	Enter a text string up to 16 characters long as the name of the peer group.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information After you configure a peer group as passive, you must assign it a subnet using the `neighbor subnet` command.

Related Commands neighbor subnet – assigns a subnet to a dynamically configured BGP neighbor.

neighbor remote-as

Create and specify the remote peer to the BGP neighbor.

S5000

Syntax `neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} remote-as `*`number`*

To delete a remote AS entry, use the `no neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} remote-as `*`number`* command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter a text string up to 16 characters long as the name of the peer group.
number	Enter a number of the AS. The range is 1 to 65535.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If the `number` parameter is the same as the AS number used in the `router bgp` command, the remote AS entry in the neighbor is considered an internal BGP peer entry.

This command creates a peer and the newly created peer is disabled (`shutdown`).

Related Commands	router bgp – enters the ROUTER BGP mode and configure routes in an AS.

neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

S5000

Syntax

`neighbor {ipv6-address | peer-group-name} remove-private-as`

To return to the default, use the `no neighbor {ipv6-address | peer-group-name} remove-private-as` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to remove the private AS numbers.

Defaults Disabled (that is, the private AS number are not removed).

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Applies to external border gateway protocol (EBGP) neighbors only.

If the AS-PATH contains both public and private AS number or contains AS numbers of an EBGP neighbor, the private AS numbers are not removed.

If a confederation contains private AS numbers in its AS-PATH, the software removes the private AS numbers only if they follow the confederation numbers in the AS path.

Private AS numbers are 64512 to 65535.

neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

S5000

Syntax

`neighbor {ipv6-address | peer-group-name} route-map map-name {in | out}`

To remove the route map, use the `no neighbor {ipv6-address | peer-group-name} route-map map-name {in | out}` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
map-name	Enter the name of an established route map. If the Route map is not configured, the default is **deny** (to drop all routes).
in	Enter the keyword `in` to filter inbound routes.
out	Enter the keyword `out` to filter outbound routes.

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

Configure a neighbor as a member of a route reflector cluster.

S5000

Syntax

```
neighbor {ipv6-address | peer-group-name} route-reflector-
client
```

To indicate that the neighbor is not a route reflector client or to delete a route reflector configuration, use the `no neighbor {ipv6-address | peer-group-name} route-reflector-client` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults Not configured.

Command Modes
ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The first time you enter this command it configures the neighbor as a route reflector and members of the route-reflector cluster. Internal BGP (IBGP) speakers do not need to be fully meshed if you configure a route reflector.

When all clients of a route reflector are disabled, the neighbor is no longer a route reflector.

neighbor send-community

Send a COMMUNITY attribute to a BGP neighbor or peer group. A COMMUNITY attribute indicates that all routes with that attribute belong to the same community grouping.

S5000

Syntax
`neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} send-community`

To disable sending a COMMUNITY attribute, use the `no neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} send-community` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults
Not configured and COMMUNITY attributes are not sent to neighbors.

Command Modes
ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

neighbor shutdown

Disable a BGP neighbor or peer group.

S5000

Syntax
`neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} shutdown`

To enable a disabled neighbor or peer group, use the `no neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} shutdown` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults Enabled (that is, BGP neighbors and peer groups are disabled.)

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Peers that are enabled within a peer group are disabled when their peer group is disabled.

The `neighbor shutdown` command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the specified BGP sessions. When a neighbor or peer group is shutdown, use the `show ip bgp ipv6 unicast summary` command to confirm its status.

Related Commands

show ip bgp ipv6 unicast summary – displays the current BGP configuration.

show ip bgp ipv6 unicast neighbors – displays IPv6 routing information exchanged by BGP neighbors.

neighbor soft-reconfiguration inbound

Enable a BGP soft-reconfiguration and start storing updates for inbound IPv6 unicast routes.

S5000

Syntax

```
neighbor {ipv4-address | ipv6-address | peer-group-name} soft-
reconfiguration inbound
```

Parameters

ipv4-address | *ipv6-address*	Enter the IP address of the neighbor for which you want to start storing inbound routing updates.
peer-group-name	Enter the name of the peer group for which you want to start storing inbound routing updates.

Defaults Disabled.

Command Modes ROUTER BGPv6 ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	This command enables soft-reconfiguration for the specified BGP neighbor. BGP stores all updates for inbound IPv6 unicast routes received by the neighbor but does not reset the peer-session. ⚠ **CAUTION: Inbound update storage is a memory-intensive operation. The entire BGP update database from the neighbor is stored in memory regardless of the inbound policy results applied on the neighbor.**
Related Commands	show ip bgp ipv6 unicast neighbors – displays IPv6 routing information exchanged by BGP neighbors.

neighbor subnet

Enable passive peering so that the members of the peer group are dynamic.

S5000

Syntax

`neighbor peer-group-name subnet subnet-number mask`

To remove passive peering, use the `no neighbor peer-group-name subnet subnet-number mask` command.

Parameters

subnet-number	Enter a subnet number in dotted decimal format (A.B.C.D.) as the allowable range of addresses included in the Peer group. To allow all addresses, enter `0::0/0`.
mask	Enter a prefix mask in / prefix-length format (/x).

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

neighbor timers

Set keepalive and hold time timers for a BGP neighbor or a peer group.

S5000

Syntax

`neighbor {ipv6-address | peer-group-name} timers keepalive holdtime`

To return to the default values, use the `no neighbor {ipv6-address | peer-group-name} timers` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the timers for all routers within the peer group.
keepalive	Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. the range is 1 to 65535. the default is **60 seconds**.
holdtime	Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. The range is 3 to 65535. The default is **180 seconds**.

Defaults

- keepalive = **60 seconds**
- holdtime = **180 seconds**

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Timer values configured with the `neighbor timers` command override the timer values configured with the `timers bgp` command.

When two neighbors, configured with different keepalive and holdtime values, negotiate for new values, the resulting values are as follows:

- the lower of the holdtime values is the new holdtime value
- whichever is the lower value; one-third of the new holdtime value, or the configured keepalive value is the new keepalive value

neighbor update-source

Enable the S5000 software to use Loopback interfaces for TCP connections for BGP sessions.

S5000

Syntax

```
neighbor {ipv6-address | peer-group-name} update-source
loopback interface
```

To use the closest interface, use the `no neighbor {ipv6-address | peer-group-name} update-source loopback interface` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

peer-group-name	Enter the name of the peer group to set the timers for all routers within the peer group.
loopback *interface*	Enter the keyword `loopback` followed by a number of the loopback interface. The range is 0 to 16383.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The `neighbor update-source` command is not necessary for directly connected internal BGP sessions.

neighbor weight

Assign a weight to the neighbor connection, which is used to determine the best path.

S5000

Syntax `neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} weight `*`weight`*

To remove a weight value, use the `no neighbor {`*`ipv6-address`*` | `*`peer-group-name`*`} weight `*`weight`* command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the timers for all routers within the peer group.
weight	Enter a number as the weight. The range is 0 to 65535. The default is **0**.

Defaults 0

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information In the FTOS best path selection process, the path with the highest weight value is preferred.

NOTE: Reset the neighbor connection (the `capture bgp-pdu max-buffer-size *` command) to apply the weight to the connection and recompute the best path.

neighbor X:X:X::X password

Enable TCP MD5 Authentication for an IPv6 BGP peer session.

S5000

Syntax

```
neighbor x:x:x::x password {7 <encrypt-pass> | <clear-pass}
```

To return to the default setting, use the `no neighbor x:x:x::x password` command.

Parameters

encrypt-pass	Enter the encrypted password.
clear-pass	Enter the clear text password.

Defaults Disabled.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The TCP session is authentication and prevents the data from being compromised.

network

Specify the networks for the BGP process and enter them in the BGP routing table.

S5000

Syntax

```
network ipv6-address prefix-length [route-map map-name]
```

To remove a network, use the `no network ip-address mask [route-map map-name]` command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
mask	Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).

route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source • set ipv6 next-hop If the route map is not configured, the default is **deny** (to drop all routes).

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands redistribute – redistributes routes into BGP.

network backdoor

Specify this IGP route as the preferred route.

S5000

Syntax `network` *`ipv6-address prefix-length`* `backdoor`

To remove a network, use the `no network` *`ipv6-address prefix-length`* `backdoor` command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Though FTOS does not generate a route due to backdoor config, there is an option for injecting/sourcing a local route in presence of network backdoor config on a learned route.

redistribute

Redistribute routes into BGP.

S5000

Syntax	`redistribute {connected | static} [route-map map-name]` To disable redistribution, use the `no redistribution {connected | static}` command.
Parameters	

connected	Enter the keyword `connected` to redistribute routes from physically connected interfaces.
static	Enter the keyword `static` to redistribute manually configured routes. These routes are treated as incomplete routes.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source • set ipv6 next-hop If the route map is not configured, the default is **deny** (to drop all routes).

Defaults	Not configured.
Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	If you do not configure the `default-metric` command, in addition to the `redistribute` command, or there is no route map to set the metric, the metric for redistributed static and connected is “0”. To redistribute the default route (`0::0/0`), configure the `neighbor default-originate` command.
Related Commands	neighbor default-originate – injects the default route.

redistribute isis

Redistribute IS-IS routes into BGP.

S5000

Syntax	`redistribute isis [level-1	level-1-2	level-2] [metric` *`metric-value`* `| metric-type {external	internal}] [route-map` *`map-name`*`]` To stop redistribution of IS-IS routes, use the `no redistribute isis` command.
Parameters	

level-1 | level-1-2 | level-2]	(OPTIONAL) Enter the type (level) of routes to redistribute.
metric	(OPTIONAL) Assign metric to an interface for use with IPv6 information.
metric-type	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. You must specify one of the following: • external • **internal** (default)
route-map ***map-name***	(OPTIONAL) Enter the keywords `route-map` followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source • set ipv6 next-hop If the route map is not configured, the default is **deny** (to drop all routes).

Defaults	Not configured.
Command Modes	ROUTER BGPV6-ADDRESS FAMILY
Command History	

Version 9.0(1.3)	Introduced on the S5000.

redistribute ospf

Redistribute OSPFv3 routes into BGP.

S5000

Syntax

```
redistribute ospf process-id [[match external {1 | 2}] [match
internal]] [route-map map-name]
```

To stop redistribution of OSPF routes, use the `no redistribute ospf process-id` command.

Parameters

process-id	Enter the number of the OSPFv3 process. The range is 1 to 65535.
match external {1 | 2}	(OPTIONAL) Enter the keywords `match external` to redistribute OSPF external routes. You can specify `1` or `2` to redistribute those routes only.
match internal	(OPTIONAL) Enter the keywords `match internal` to redistribute OSPFv3 internal routes only.
route-map ***map-name***	(OPTIONAL) Enter the keywords `route-map` followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source • set ipv6 next-hop If the route map is not configured, the default is **deny** (to drop all routes).

Defaults

Not configured.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you enter the `redistribute ospf process-id` command without any other parameters, FTOS redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes.

router bgp

Enter ROUTER BGP mode to configure and enable BGP.

S5000

Syntax

`router bgp as-number`

To disable BGP, use the `no router bgp as-number` command.

Parameters

as-*number*	Enter the AS number. The range is 1 to 65535.

Defaults

Not enabled.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

show capture bgp-pdu neighbor

Display BGP packet capture information for an IPv6 address on the S5000.

S5000

Syntax

`show capture bgp-pdu neighbor ipv6-address`

Parameters

ipv6-address	Enter the IPv6 address (X:X:X:X::X) of a BGP neighbor.

Defaults

- EXEC
- EXEC Privilege

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Command

capture bgp-pdu neighbor (ipv6) – enables capture of an IPv6 BGP neighbor packet.

capture bgp-pdu max-buffer-size – specifies a size for the capture buffer.

show config

View the current ROUTER BGP configuration.

S5000

Syntax `show config`

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Example

```
FTOS(conf-router_bgp)#show conf
!
router bgp 18508
 neighbor RR-CLIENT peer-group
 neighbor RR-CLIENT remote-as 18508
 neighbor RR-CLIENT no shutdown
 neighbor RR-CLIENT-PASSIV peer-group passive
 neighbor RR-CLIENT-PASSIV remote-as 18508
 neighbor RR-CLIENT-PASSIV subnet 9000::9:0/120
 neighbor RR-CLIENT-PASSIV no shutdown
 neighbor 1109::33 remote-as 18508
 neighbor 1109::33 update-source Loopback 101
 neighbor 1109::33 no shutdown
 neighbor 2222::220 remote-as 18508
 neighbor 2222::220 route-reflector-client
 neighbor 2222::220 update-source Loopback 100
 neighbor 2222::220 no shutdown
 neighbor 4000::33 remote-as 18508
 neighbor 4000::33 no shutdown
 neighbor 4000::60 remote-as 18508
 neighbor 4000::60 no shutdown
 neighbor 9000::1:2 remote-as 640
 no neighbor 9000::1:2 activate
 neighbor 9000::1:2 no shutdown

!
FTOS#
```

show ip bgp ipv6 unicast

View the current BGP information.

S5000

Syntax `show ip bgp ipv6 unicast [`*`network`*` [`*`network-mask`*`] [longer-prefixes]]`

Paramters

network	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
network-mask	(OPTIONAL) Enter the keywords `network mask` (in slash prefix format) of the BGP network address.

longer-prefixes	(OPTIONAL) Enter the keywords `longer-prefixes` to view all routes with a common prefix.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you enable `bgp non-deterministic-med` command, the `show ip bgp` command output for a BGP route does not list the INACTIVE reason.

show ip bgp ipv6 unicast cluster-list

View BGP neighbors in a specific cluster.

S5000

Syntax

`show ip bgp ipv6 unicast cluster-list [cluster-id]`

Paramters

cluster-id	(OPTIONAL) Enter the cluster id in dotted decimal format.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp ipv6 unicast community

View information on all routes with community attributes or view specific BGP community groups.

S5000

Syntax

```
show ip bgp ipv6 unicast community [community-number] [local-
as] [no-export] [no-advertise]
```

Paramters

community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.

local-AS	Enter the keywords `local-AS` to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords `no-advertise` to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords `no-export` to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp ipv6 unicast summary` command. The text line above the route table states the number of COMMUNITY attributes found.

show ip bgp ipv6 unicast community-list

View routes that are affected by a specific community list.

S5000

Syntax

```
show ip bgp ipv6 unicast community-list community-list-name
[exact-match]
```

Paramters

community-list-name	Enter the name of a configured IP community list.
exact-match	(OPTIONAL) Enter the keywords `exact-match` to display only for an exact match of the communities.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp ipv6 unicast dampened-paths

View BGP routes that are dampened (non-active).

S5000

Syntax	`show ip bgp ipv6 unicast dampened-paths`
Command Modes	• EXEC • EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

show ip bgp ipv6 unicast detail

Display BGP internal information for IPv6 Unicast address family.

S5000

Syntax	`show ip bgp ipv6 unicast detail`
Defaults	none
Command Modes	• EXEC • EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

show ip bgp ipv6 unicast extcommunity-list

View information on all routes with Extended Community attributes.

S5000

Syntax	`show ip bgp ipv6 unicast extcommunity-list [list name]`
Parameters	*list name* Enter the extended community list name you wish to view.
Command Modes	• EXEC • EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp ipv6 unicast summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp ipv6 unicast community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp ipv6 unicast` command output.

show ip bgp ipv6 unicast filter-list

View the routes that match the filter lists.

S5000

Syntax

```
show ip bgp ipv6 unicast filter-list as-path-name
```

Parameters

as-path-name	Enter the name of an AS-PATH.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp ipv6 unicast flap-statistics

View flap statistics on BGP routes.

S5000

Syntax

```
show ip bgp ipv6 unicast flap-statistics [ipv6-address prefix-
length] [filter-list as-path-name] [regexp regular-expression]
```

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

filter-list *as-path-name*	(OPTIONAL) Enter the keywords `filter-list` followed by the name of a configured AS-PATH ACL.
regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match: • `.` = (period) any single character (including a white space). • `*` = (asterisk) the sequences in a pattern (0 or more sequences). • `+` = (plus) the sequences in a pattern (1 or more sequences). • `?` = (question mark) sequences in a pattern (either 0 or 1 sequences). **NOTE:** You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression. • `[ ]` = (brackets) a range of single-character patterns. • `^` = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified. • `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp ipv6 unicast inconsistent-as

View routes with inconsistent originating autonomous system (AS) numbers; that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

S5000

Syntax `show ip bgp ipv6 unicast inconsistent-as`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp ipv6 unicast neighbors

Displays information on IPv6 unicast routes exchanged by BGP neighbors.

S5000

Syntax

```
show ip bgp ipv6 unicast neighbors [ipv4-neighbor-addr | ipv6-
neighbor-addr] [advertised-routes | dampened-routes | detail |
flap-statistics | routes | received-routes [network [network-
mask]] | denied-routes [network [network-mask]]]
```

Parameters

ipv6 unicast	Enter the keywords `ipv6 unicast` to view information only related to IPv6 unicast routes.
ipv4-neighbor-addr | *ipv6-neighbor-addr*	(OPTIONAL) Enter the IP address of the neighbor to view only BGP route information exchanged with that neighbor.
advertised-routes	(OPTIONAL) Enter the keywords `advertised-routes` to view only the routes the neighbor sent.
dampened-routes	(OPTIONAL) Enter the keywords `dampened-routes` to view information on dampened routes from the BGP neighbor.
detail	(OPTIONAL) Enter the keyword `detail` to view neighbor-specific internal information for the IPv4 Unicast address family.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to view flap statistics on the neighbor's routes.
routes	(OPTIONAL) Enter the keyword `routes` to view only the neighbor's feasible routes.
received-routes [*network* [*network-mask*]	(OPTIONAL) Enter the keywords `received-routes` followed by either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information received from neighbors. **NOTE:** The `neighbor soft-reconfiguration inbound` command must be configured prior to viewing all the information received from the neighbors.
denied-routes [*network* [*network-mask*]	(OPTIONAL) Enter the keywords `denied-routes` followed by either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information on routes denied using neighbor inbound filters.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp ipv6 unicast neighbors` command shown in the Example below.

Lines Beginning with	Description
BGP neighbor	Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, then the link is internal; otherwise, the link is external.
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information: • last read is the time (hours:minutes:seconds) the router reads a message from its neighbor • hold time is the number of seconds configured between messages from its neighbor • keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive
Received messages	This line displays the number of BGP messages received, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Sent messages	The line displays the number of BGP messages sent, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Received updates	This line displays the number of BGP updates received and sent.
Soft reconfiguration	This line indicates that soft reconfiguration inbound is configured.
Minimum time	Displays the minimum time, in seconds, between advertisements.
(List of inbound and outbound policies)	Displays the policy commands configured and the names of the Route map, AS-PATH ACL, or Prefix list configured for the policy.
For address family:	Displays IPv6 Unicast as the address family.
BGP table version	Displays which version of the primary BGP routing table the router and the neighbor are using.
Prefixes accepted	Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.
Prefixes advertised	Displays the number of network prefixes advertised, the number rejected, and the number withdrawn from the BGP routing table.

Connections established	Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.
Last reset	Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word "never" is displayed.
Local host:	Displays the peering address of the local router and the TCP port number.
Foreign host:	Displays the peering address of the neighbor and the TCP port number.

Example

```
FTOS#show ip bgp ipv6 unicast neighbors

BGP neighbor is 5ffe:10::3, remote AS 1, external link
  BGP version 4, remote router ID 5.5.5.3
  BGP state ESTABLISHED, in this state for 00:00:32
  Last read 00:00:32, last write 00:00:32
  Hold time is 180, keepalive interval is 60 seconds
  Received 1404 messages, 0 in queue
    3 opens, 1 notifications, 1394 updates
    6 keepalives, 0 route refresh requests
  Sent 48 messages, 0 in queue
    3 opens, 2 notifications, 0 updates
    43 keepalives, 0 route refresh requests
  Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds

  Capabilities received from neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  Capabilities advertised to neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  For address family: IPv6 Unicast
  BGP table version 12, neighbor version 12
  2 accepted prefixes consume 32 bytes

  Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
  Prefixes advertised 0, rejected 0, withdrawn 0 from peer
  Connections established 3; dropped 2
  Last reset 00:00:39, due to Closed by neighbor

  Notification History
    'OPEN error/Bad AS' Sent : 0 Recv: 1

  Local host: 5ffe:10::4, Local port: 179
  Foreign host: 5ffe:10::3, Foreign port: 35470

  Notification History
    'Connection Reset' Sent : 1 Recv: 0

  BGP neighbor is 5ffe:11::3, remote AS 1, external link
    BGP version 4, remote router ID 5.5.5.3
    BGP state ESTABLISHED, in this state for 00:00:28
    Last read 00:00:28, last write 00:00:28
    Hold time is 180, keepalive interval is 60 seconds
    Received 27 messages, 3 notifications, 0 in queue
    Sent 0 messages, 0 notifications, 0 in queue
    Received 8 updates, Sent 0 updates
    Route refresh request: received 0, sent 0
    Minimum time between advertisement runs is 30 seconds
    Minimum time before advertisements start is 0 seconds

  Capabilities received from neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)
    Capabilities advertised to neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  For address family: IPv6 Unicast
  BGP table version 12, neighbor version 12
  2 accepted prefixes consume 32 bytes

  Prefix advertised 0, rejected 0, withdrawn 0
  Connections established 3; dropped 2
  Last reset 00:00:41, due to Closed by neighbor

  Notification History
    'OPEN error/Bad AS' Sent : 0 Recv: 1

Local host: 5ffe:11::4, Local port: 179
```

Related Commands show ip bgp ipv6 unicast – views the current BGP routing table.

show ip bgp ipv6 unicast peer-group

Allows you to view information on the BGP peers in a peer group.

S5000

Syntax `show ip bgp ipv6 unicast peer-group [`*`peer-group-name`*` [summary]]`

Parameters

peer-group-name	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
detail	(OPTIONAL) Enter the keyword `detail` to view peer-group-specific information for the IPv6 address family.
summary	(OPTIONAL) Enter the keyword `summary` to view status information of the peers in that peer group. The output is the same as that found in the `show ip bgp ipv6 unicast summary` command.

Command Modes

- EXEC
- EXEC Privilege

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip bgp peer-group

Peer-group RR-CLIENT, remote AS 18508
  BGP version 4
  Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
  BGP neighbor is RR-CLIENT, peer-group internal,
  Number of peers in this group 1
  Peer-group members (* - outbound optimized):
    9000::4:

Peer-group RR-CLIENT-PASSIV, remote AS 18508
  BGP version 4
  Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
  BGP neighbor is RR-CLIENT-PASSIV, peer-group internal,
  Number of peers in this group 1
  Peer-group members (* - outbound optimized):
    9000::9:2*
FTOS#
```

show ip bgp ipv6 unicast summary

Allows you to view the status of all BGP connections.

S5000

Syntax `show ip bgp ipv6 unicast summary`

Command Modes

- EXEC
- EXEC Privilege

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS# show ip bgp summary
BGP router identifier 55.55.55.55, local AS number 18508
BGP table version is 0, main routing table version 0
6 BGP path attribute entrie(s) using 392 bytes of memory
6 BGP AS-PATH entrie(s) using 294 bytes of memory
6 BGP community entrie(s) using 234 bytes of memory

Neighbor  AS    MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/
Pfx

1109::33   18508 0       0       0      0     0   never  Active
2222::220  18508 0       0       0      0     0   never  Active
4000::33   18508 0       0       0      0     0   never  Active
4000::60   18508 0       0       0      0     0   never  Active
```

```
9000::4:2  18508 0       0       0      0     0   never  Active
9000::5:2  1     35      32      0      0     0   00:16:42    0
9000::6:2  2     35      32      0      0     0   00:16:39    0
9000::7:2  3     35      32      0      0     0   00:16:41    0
9000::8:2  18508 35      32      0      0     0   00:16:42    0
9000::9:2  18508 44      19      0      0     0   00:16:41    0
9000::a:2  18508 35      32      0      0     0   00:16:43    0
9000::b:14 18508 29      29      0      0     0   00:13:01    0
FTOS#
```

show ip bgp next-hop

View all next hops (using learned routes only) with current reachability and flap status. This command only displays one path, even if the next hop is reachable by multiple paths.

S5000

Syntax

```
show ip bgp next-hop [local-routes]
```

Parameters

local-routes	(OPTIONAL) Show next-hop information for local routes.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip bgp next-hop
Next-hop   Via               RefCount Cost Flaps Time Elapsed
9000::5:2  9000::5:2, Te 8/38  2        0    0   00:23:22
9000::6:2  9000::6:2, Te 8/38  2        0    0   00:23:22
9000::7:2  9000::7:2, Te 8/38  2        0    0   00:23:22
9000::8:2  9000::8:2, Te 8/38  2        0    0   00:23:22
9000::9:2  9000::9:2, Te 8/38  6000     0    0   00:23:16
9000::a:2  9000::a:2, Te 8/38  2        0    0   00:23:22
FTOS#
```

show ip bgp paths

View all the BGP path attributes in the BGP database.

S5000

Syntax

```
show ip bgp paths [regexp regular-expression]
```

Parameters		
	regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match: • `.` = (period) any single character (including a white space). • `*` = (asterisk) the sequences in a pattern (0 or more sequences). • `+` = (plus) the sequences in a pattern (1 or more sequences). • `?` = (question mark) sequences in a pattern (either 0 or 1 sequences). **NOTE:** You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression. • `[ ]` = (brackets) a range of single-character patterns. • `^` = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified. • `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp paths as-path

View all unique AS-PATHs in the BGP database.

S5000

Syntax

```
show ip bgp paths as-path
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp paths community

View all unique COMMUNITY numbers in the BGP database.

S5000

Syntax `show ip bgp paths community`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp paths extcommunity

View all unique extended community information in the BGP database.

S5000

Syntax `show ip bgp paths extcommunity`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on theS5000.

show ip bgp regexp

Allows you to view the subset of BGP routing table matching the regular expressions specified.

S5000

Syntax `show ip bgp regexp` *`regular-expression`* `[`*`character`*`]`

Parameters

***regular-expression* [*character*]**	Enter a regular expression then use one or a combination of the following characters to match: • `.` = (period) any single character (including a white space). • `*` = (asterisk) the sequences in a pattern (0 or more sequences).

- `+` = (plus) the sequences in a pattern (1 or more sequences).
- `?` = (question mark) sequences in a pattern (either 0 or 1 sequences).

  NOTE: You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression.
- `[ ]` = (brackets) a range of single-character patterns.
- `^` = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

timers bgp

Allows you to adjust the BGP network timers for all neighbors.

S5000

Syntax

`timers bgp` *`keepalive holdtimer`*

To return to the default values, use the `no timers bgp` command.

Parameters

keepalive	Enter the time interval (in seconds) between keepalive messages. The range is 1 to 65535. The default is **60 seconds**.
holdtimer	Enter the time interval (in seconds) that the S5000 waits since the last keepalive message before declaring a BGP peer dead. The range is 3 to 65535. The default is **180 seconds**.

Defaults

- keepalive = **60 seconds**
- holdtimer = **180 seconds**

Command Modes ROUTER BGP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands neighbor timers – adjusts BGP timers for a specific peer or peer group.

IPv6 MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the Internet and connecting multicast topologies between BGP and autonomous systems (AS). The Dell Networking operating software (FTOS) MBGP is implemented as per IETF RFC 1858.

address family

This command changes the context to subsequent address family identifier (SAFI).

S5000

Syntax

`address family ipv6 unicast`

To remove SAFI context, use the `no address family ipv6 unicast` command.

Parameters

ipv6	Enter the keyword `ipv6` to specify the address family as IPv6.
unicast	Enter the keyword `unicast` to specify multicast as SAFI.

Defaults

IPv6 Unicast

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

After this command is executed, all subsequent commands apply to this address family. You can exit from this AFI/SAFI to the IPv6 Unicast (the default) family by entering the `exit` command and returning to the Router BGP context.

aggregate-address

Summarize a range of prefixes to minimize the number of entries in the routing table.

S5000

Syntax

`aggregate-address` *`ipv6-address prefix-length`* `[advertise-map` *`map-name`*`] [as-set] [attribute-map` *`map-name`*`] [summary-only] [suppress-map` *`map-name`*`]`

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the / x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

advertise-map *map-name*	(OPTIONAL) Enter the keywords `advertise-map` followed by the name of a configured route map to set filters for advertising an aggregate route.
as-set	(OPTIONAL) Enter the keywords `as-set` to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.
attribute-map *map-name*	(OPTIONAL) Enter the keywords `attribute-map` followed by the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
summary-only	(OPTIONAL) Enter the keywords `summary-only` to advertise only the aggregate address. Specific routes are not advertised.
suppress-map *map-name*	(OPTIONAL) Enter the keywords `suppress-map` followed by the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

Defaults

Not configured.

Command Modes

ROUTER-BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

Do not add the `as-set` parameter to the aggregate. If routes within the aggregate are constantly changing, the aggregate flaps to keep track of the changes in the AS_PATH.

In route maps used in the `suppress-map` parameter, routes meeting the `deny` clause are not suppress; in other words, they are allowed. The opposite is true: routes meeting the `permit` clause are suppressed.

If the route is injected using the `network` command, that route stills appear in the routing table if the `summary-only` parameter is configured in the `aggregate-address` command.

The `summary-only` parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the `neighbor distribute-list` command.

bgp dampening

Enable BGP route dampening and configure the dampening parameters.

S5000

Syntax

```
bgp dampening [half-life reuse suppress max-suppress-time]
[route-map map-name]
```

Parameters

half-life	(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half, after the half-life period expires. The range is 1 to 45. The default is **15 minutes**.
reuse	(OPTIONAL) Enter a number as the reuse value, which is compared to the flapping route's Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed). The range is 1 to 20000. The default is **750**.
suppress	(OPTIONAL) Enter a number as the suppress value, which is compared to the flapping route's Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed). The range is 1 to 20000. The default is **2000**.
max-suppress-time	(OPTIONAL) Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value. The range is 1 to 255. The default is **60 minutes**.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of a configured route map. Only match commands in the configured route map are supported.

Defaults

Disabled.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you enter `bgp dampening`, the default values for `half-life`, `reuse`, `suppress`, and `max-suppress-time` are applied. The parameters are position-dependent; therefore, if you configure one parameter, you must configure the parameters in the order they appear in the command.

Related Commands

show ip bgp ipv6 unicast dampened-paths – views the BGP paths.

clear ip bgp ipv6 unicast

Reset MBGP sessions.

S5000

Syntax

```
clear ip bgp ipv6 unicast * ipv6-address prefix-length
[dampening | flap-statistics] peer-group]
```

Parameters

*****	Enter the character `*` to clear all peers.

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
dampening	(OPTIONAL) Enter the keyword `dampening` to clear route flap dampening information.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to reset the flap statistics on all prefixes from that neighbor.
peer-group	(OPTIONAL) Enter the keywords `peer-group` to clear all members of a peer-group.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ip bgp ipv6 unicast dampening

Clear information on route dampening.

S5000

Syntax

```
clear ip bgp dampening ipv6 unicast [network network-mask]
```

Parameters

network	(OPTIONAL) Enter the IPv6 network address in x:x:x:x::x format.
network-mask	If you enter the network address, next enter the network mask, from 0 to 128.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ip bgp ipv6 flap-statistics

Clear BGP flap statistics, which includes the number of flaps and the time of the last flap.

S5000

Syntax

```
clear ip bgp ipv6 unicast flap-statistics [network | filter-
list list |regexp regexp
```

Parameters

network	(OPTIONAL) Enter the IPv6 network address in x:x:x:x::x format to clear flap statistics.
filter-list *list*	(OPTIONAL) Enter the keywords `filter-list` followed by the name of a configured AS-PATH list (maximum 16 characters).
regexp *regexp*	(OPTIONAL) Enter the keyword `regexp` followed by regular expressions. Use one or a combination of the following: • `.` (period) matches on any single character, including white space. • `*` (asterisk) matches on sequences in a pattern (zero or more sequences). • `+` (plus sign) matches on sequences in a pattern (one or more sequences). • `?` (question mark) matches sequences in a pattern (0 or 1 sequences). • `[ ]` (brackets) matches a range of single-character patterns. • `^` (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.) • `$` (dollar sign) matches the end of the output string.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug ip bgp ipv6 unicast dampening

View information on routes being dampened.

S5000

Syntax

```
debug ip bgp ipv6 unicast dampening
```

To disable debugging, use the `no debug ip bgp ipv6 unicast dampening` command.

Parameters

dampening	Enter the keyword `dampening` to clear route flap dampening information.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug ip bgp ipv6 unicast peer-group updates

View information about BGP peer-group updates.

S5000

Syntax

```
debug ip bgp ipv6 unicast peer-group peer-group-name updates
[in | out]
```

To disable debugging, use the `no debug ip bgp ipv6 unicast peer-group peer-group-name updates [in | out]` command.

Parameters

peer-group *peer-group-name*	Enter the keywords `peer-group` followed by the name of the peer-group.
updates	Enter the keyword `updates` to view BGP update information.
in	(OPTIONAL) Enter the keyword `in` to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view only BGP updates sent to neighbors.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug ip bgp ipv6 unicast updates

View information about BGP updates.

S5000

Syntax

```
debug ip bgp ipv6 unicast ipv6-address prefix-length updates
[in | out]
```

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
updates	Enter the keyword `updates` to view BGP update information.
in	(OPTIONAL) Enter the keyword `in` to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view only BGP updates sent to neighbors.

Defaults	Disabled.
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

distance bgp

Define an administrative distance for routes.

S5000

Syntax

`distance bgp external-distance internal-distance local-distance`

To return to default values, use the `no distance bgp` command.

Parameters

external-distance	Enter a number to assign to routes learned from a neighbor external to the AS. The range is 1 to 255. The default is **20**.
internal-distance	Enter a number to assign to routes learned from a router within the AS. The range is 1 to 255. The default is **200**.
local-distance	Enter a number to assign to routes learned from networks listed in the network command. The range is 1 to 255. The default is **200**.

Defaults

- external-distance = **20**
- internal-distance = **200**
- local-distance = **200**

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

CAUTION: Dell Networking recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table.

Routes from confederations are treated as internal BGP routes.

neighbor activate

Allows you to enable a specified neighbor/peer group for the current address and subsequent address family identifier (AFI/SAFI).

S5000

Syntax

`neighbor [ipv6-address | peer-group-name] activate`

To disable, use the `no neighbor [ipv6-address | peer-group-name] activate` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Identify a peer group by name.
activate	Enter the keyword `activate` to enable the identified neighbor or peer group in the new AFI/SAFI.

Defaults

Disabled.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

By default, when a neighbor/peer group configuration is created in the Router BGP context, it is enabled for the IPv6/Unicast AFI/SAFI. By using `activate` in the new context, the neighbor/peer group is enabled for AFI/SAFI.

Related Command

address family – changes the context to SAFI.

neighbor advertisement-interval

Set the advertisement interval between BGP neighbors or within a BGP peer group.

S5000

Syntax

`neighbor {ipv6-address | peer-group-name} advertisement-interval seconds`

To return to the default value, use the `no neighbor {ipv6-address | peer-group-name} advertisement-interval` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
seconds	Enter a number as the time interval, in seconds, between BGP advertisements. The range is 0 to 600 seconds. The default is **5 seconds** for internal BGP peers and **30 seconds** for external BGP peers.

Defaults

- seconds = **5 seconds** (internal peers)
- seconds = **30 seconds** (external peers)

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

neighbor default-originate

Inject the default route to a BGP peer or neighbor.

S5000

Syntax

```
neighbor {ipv6-address | peer-group-name} default-originate
[route-map map-name]
```

To remove a default route, use the `no neighbor {ipv6-address | peer-group-name} default-originate` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the default route of all routers in that peer group.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

neighbor distribute-list

Distribute BGP information using an established prefix list.

S5000

Syntax

`neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}`

To delete a neighbor distribution list, use the `no neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
prefix-list-name	Enter the name of an established prefix list. If the prefix list is not configured, the default is **permit** (to allow all routes).
in	Enter the keyword in to distribute only inbound traffic.
out	Enter the keyword out to distribute only outbound traffic.

Defaults

Not configured.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

neighbor filter-list – assigns a AS-PATH list to a neighbor or peer group.

neighbor route-map – assigns a route map to a neighbor or peer group.

neighbor filter-list

Configure a BGP filter based on the AS-PATH attribute.

S5000

Syntax

`neighbor [ipv6-address | peer-group-name] filter-list aspath access-list-name [in | out]`

To delete a BGP filter, use the `no neighbor [ipv6-address | peer-group-name] filter-list aspath access-list-name [in | out]` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

peer-group-name	Enter the name of the peer group to apply the filter to all routers in the peer group.
access-list-name	Enter the name of an established AS-PATH access list. If the AS-PATH access list is not configured, the default is **permit** (to allow routes).
in	Enter the keyword `in` to filter inbound BGP routes.
out	Enter the keyword `out` to filter outbound BGP routes.

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

neighbor maximum-prefix

Control the number of network prefixes received.

S5000

Syntax

```
neighbor {ipv6-address | peer-group-name} maximum-prefix
maximum [threshold] [warning-only]
```

To return to the default values, use the `no neighbor {ipv6-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
maximum	Enter a number as the maximum number of prefixes allowed for this BGP router. The range is 1 to 4294967295.
threshold	(OPTIONAL) Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches this threshold, the software sends a message. The range is 1 to 100 percent. The default is **75**.
warning-only	(OPTIONAL) Enter the keyword `warning-only` to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

Defaults threshold = **75**

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

neighbor next-hop-self

Allows you to configure the router as the next hop for a BGP neighbor.

S5000

Syntax

`neighbor {ipv6-address | peer-group-name} next-hop-self`

To return to the default setting, use the `no neighbor {ipv6-address | peer-group-name} next-hop-self` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	(OPTIONAL) Enter the name of the peer group.

Defaults Disabled.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If you configure the `set ipv6 next-hop` command in ROUTE-MAP mode, its configuration takes precedence over the `neighbor next-hop-self` command.

neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

S5000

Syntax

`neighbor {ipv6-address | peer-group-name} remove-private-as`

To return to the default, use the `no neighbor {ipv6-address | peer-group-name} remove-private-as` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format.

	NOTE: The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to remove the private AS numbers.

Defaults Disabled (that is, the private AS number are not removed).

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on theS5000.

neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

S5000

Syntax

```
neighbor {ipv6-address | peer-group-name} route-map map-name
{in | out}
```

To remove the route map, use the `no neighbor {ipv6-address | peer-group-name} route-map map-name {in | out}` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
map-name	Enter the name of an established route map. If the Route map is not configured, the default is **deny** (to drop all routes).
in	Enter the keyword `in` to filter inbound routes.
out	Enter the keyword `out` to filter outbound routes.

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

Configure a neighbor as a member of a route reflector cluster.

S5000

Syntax

`neighbor {ipv6-address | peer-group-name} route-reflector-client`

To indicate that the neighbor is not a route reflector client or to delete a route reflector configuration, use the `no neighbor {ipv6-address | peer-group-name} route-reflector-client` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults

Not configured.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The first time you enter this command it configures the neighbor as a route reflector and members of the route-reflector cluster. Internal BGP (IBGP) speakers do not need to be fully meshed if you configure a route reflector.

When all clients of a route reflector are disabled, the neighbor is no longer a route reflector.

network

Specify the networks for the BGP process and enter them in the BGP routing table.

S5000

Syntax

`network ipv6-address [route-map map-name]`

To remove a network, use the `no network ipv6-address [route-map map-name]` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source • set ipv6 next-hop If the route map is not configured, the default is **deny** (to drop all routes).

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The E-Series software resolves the network address configured by the `network` command with the routes in the main routing table to ensure that the networks are reachable using non-BGP routes and non-default routes.

Related Commands redistribute – redistributes routes into BGP.

redistribute

Redistribute routes into BGP.

S5000

Syntax `redistribute {connected | static} [route-map map-name]`

To disable redistribution, use the `no redistribution {connected | static}` command.

Parameters

connected	Enter the keyword `connected` to redistribute routes from physically connected interfaces.
static	Enter the keyword `static` to redistribute manually configured routes. These routes are treated as incomplete routes.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source

- set ipv6 next-hop

If the route map is not configured, the default is **deny** (to drop all routes).

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you do not configure the `default-metric` command, in addition to the `redistribute` command, or there is no route map to set the metric, the metric for redistributed static and connected is “0”.

To redistribute the default route (`0::0/0`), configure the `neighbor default-originate` command.

Related Commands

neighbor default-originate – injects the default route.

show ip bgp ipv6 unicast

View the current MBGP route table.

S5000

Syntax

```
show ip bgp ipv6 unicast [network [network-mask] [length]]
```

Paramters

network	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
network-mask	(OPTIONAL) Enter the keywords `network mask` (in slash prefix format) of the BGP network address.
longer-prefixes	(OPTIONAL) Enter the keywords `longer-prefixes` to view all routes with a common prefix.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp ipv6 unicast` command shown in the Example below.

Field	**Description**

Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0::0/0 is listed in this column, local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
FTOS#show ip bgp ipv6 unicast
BGP table version is 8, local router ID is 5.5.10.4
Status codes: s suppressed, S stale, d damped, h history, *
valid, > best Path source: I - internal, a
- aggregate, c - confed-external, r - redistributed, n -
network Origin codes: i - IGP, e - EGP, ? -
incomplete

   Network Next Hop         Metric LocPrf Weight Path
h  dead:1::/100 5ffe:10::3     0               0 1 i
h               5ffe:11::3     0               0 1 i
*> dead:2::/100 5ffe:10::3     0               0 1 i
*               5ffe:11::3     0               0 1 i
*> dead:3::/100 5ffe:10::3     0               0 1 i
*               5ffe:11::3     0               0 1 i
h  dead:4::/100 5ffe:10::3     0               0 1 i
h               5ffe:11::3     0               0 1 i
FTOS#show ip bgp ipv6 unicast dead:3::/100

BGP routing table entry for dead:3::/100, version 3
Paths: (2 available, table Default-MBGP-Routing-Table.)
Not advertised to any peer

Received from :
  5ffe:10::3 (5.5.5.3) Best
    AS_PATH : 1

    Next-Hop : 5ffe:10::3, Cost : 0
    Origin IGP, Metric 0, LocalPref 100, Weight 0, external

  5ffe:11::3 (5.5.5.3)
    AS_PATH : 1

    Next-Hop : 5ffe:11::3, Cost : 0
    Origin IGP, Metric 0, LocalPref 100, Weight 0, external
    Inactive reason: Peer IP address
FTOS#
```

Related Commands

show ip bgp ipv6 unicast community – views BGP communities.

show ip bgp ipv6 unicast cluster-list

View BGP neighbors in a specific cluster.

S5000

Syntax

```
show ip bgp ipv6 unicast cluster-list [cluster-id]
```

Paramters

cluster-id	(OPTIONAL) Enter the cluster id in dotted decimal format.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp ipv6 unicast community

View information on all routes with community attributes or view specific BGP community groups.

S5000

Syntax

```
show ip bgp ipv6 unicast community [community-number] [local-
as] [no-export] [no-advertise]
```

Paramters

community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.
local-AS	Enter the keywords `local-AS` to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords `no-advertise` to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords `no-export` to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes

- EXEC

- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp ipv6 unicast summary` command. The text line above the route table states the number of COMMUNITY attributes found.

show ip bgp ipv6 unicast community-list

View routes that are affected by a specific community list.

S5000

Syntax `show ip bgp ipv6 unicast community-list` *`community-list-name`*

Paramters

community-list-name	Enter the name of a configured IP community list.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp ipv6 unicast dampened-paths

View BGP routes that are dampened (non-active).

S5000

Syntax `show ip bgp ipv6 unicast dampened-paths`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp ipv6 unicast detail

Display detailed BGP information.

S5000

Syntax

```
show ip bgp ipv6 unicast detail
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
R2_Training#show ip bgp ipv6 unicast detail

Detail information for BGP Node
bgpNdP 0x41a17000 : NdTmrP 0x41a17000 : NdKATmrP 0x41a17014 :
NdTics 327741 :
NhLocAS 1 : NdState 2 : NdRPMPrim 1 : NdListSoc 13
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfedId 0 : NdMedConfed 0 :
NdMedMissVal -1 :
NdIgnrIllId 0 : NdRRC2C 1 : NdClstId 33686273 : NdPaTblP
0x41a19088
NdASPTblP 0x41a19090 : NdCommTblP 0x41a19098 : NhOptTransTblP
0x41a190a0 :
NdRRClsTblP 0x41a190a8
NdPktPA 0 : NdLocCBP 0x41a6f000 : NdTmpPAP 0x419efc80 :
NdTmpASPAP 0x41a25000 :
NdTmpCommP 0x41a25800
NdTmpRRClP 0x41a4b000 : NdTmpOptP 0x41a4b800 : NdTmpNHP :
NdOrigPAP 0
NdOrgNHP 0 : NdModPathP 0x419efcc0 : NdModASPAP 0x41a4c000 :
NdModCommP 0x41a4c800
NdModOptP 0x41a4d000 : NdModNHP : NdComSortBufP 0x41a19110 :
NdComSortHdP
0x41a19d04 : NdUpdAFMsk 0 : AFRstSe
t 0x41a1a298 : NHopDfrdHdP 0x41a1a3e0 : NumNhDfrd 0 :
CfgHdrAFMsk 1
```

show ip bgp ipv6 unicast filter-list

View the routes that match the filter lists.

S5000

Syntax

```
show ip bgp ipv6 unicast filter-list as-path-name
```

Parameters

as-path-name	Enter the name of an AS-PATH.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp ipv6 unicast flap-statistics

View flap statistics on BGP routes.

S5000

Syntax

```
show ip bgp ipv6 unicast flap-statistics [ipv6-address prefix-
length] [filter-list as-path-name] [regexp regular-expression]
```

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
filter-list *as-path-name*	(OPTIONAL) Enter the keywords `filter-list` followed by the name of a configured AS-PATH ACL.
regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match: • `.` = (period) any single character (including a white space). • `*` = (asterisk) the sequences in a pattern (0 or more sequences). • `+` = (plus) the sequences in a pattern (1 or more sequences). • `?` = (question mark) sequences in a pattern (either 0 or 1 sequences). **NOTE:** You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression. • `[ ]` = (brackets) a range of single-character patterns. • `^` = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified. • `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip bgp ipv6 unicast flap-statistics
BGP table version is 8, local router ID is 5.5.10.4
Status codes: s suppressed, S stale, d damped, h history, *
valid, > best Path
source: I - internal, a - aggregate, c - confed-external, r -
redistributed, n -
network Origin codes: i - IGP, e - EGP, ? - incomplete

   Network       From        Flaps  Duration Reuse Path
h  dead:1::/100  5ffe:10::3  1      00:03:20       1 i
h  dead:1::/100  5ffe:11::3  1      00:03:20       1 i
h  dead:4::/100  5ffe:10::3  1      00:04:39       1 i
h  dead:4::/100  5ffe:11::3  1      00:04:39       1 i

FTOS#
```

show ip bgp ipv6 unicast inconsistent-as

View routes with inconsistent originating autonomous system (AS) numbers; that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

S5000

Syntax

```
show ip bgp ipv6 unicast inconsistent-as
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip bgp ipv6 unicast neighbors

Allows you to view the information exchanged by BGP neighbors.

S5000

Syntax

```
show ip bgp ipv6 unicast neighbors [ipv6-address prefix-length
[advertised-routes | dampened-routes | detail | flap-statistics
| routes]]
```

Parameters

ipv6-address prefix-length	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
advertised-routes	(OPTIONAL) Enter the keywords `advertised-routes` to view only the routes the neighbor sent.
dampened-routes	(OPTIONAL) Enter the keywords `dampened-routes` to view information on dampened routes from the BGP neighbor.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to view flap statistics on the neighbor's routes.
detail	(OPTIONAL) Display detailed neighbor information.
routes	(OPTIONAL) Enter the keyword `routes` to view only the neighbor's feasible routes.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp ipv6 unicast neighbors` command shown in the Example below.

Lines Beginning with	**Description**
BGP neighbor	Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, then the link is internal; otherwise, the link is external.
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information: • last read is the time (hours:minutes:seconds) the router reads a message from its neighbor • hold time is the number of seconds configured between messages from its neighbor • keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive

Received messages	This line displays the number of BGP messages received, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Sent messages	The line displays the number of BGP messages sent, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Received updates	This line displays the number of BGP updates received and sent.
Minimum time	Displays the minimum time, in seconds, between advertisements.
(List of inbound and outbound policies)	Displays the policy commands configured and the names of the Route map, AS-PATH ACL, or Prefix list configured for the policy.
For address family:	Displays IPv6 Unicast as the address family.
BGP table version	Displays which version of the primary BGP routing table the router and the neighbor are using.
Accepted Prefixes	Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.
Prefixes advertised	Displays the number of network prefixes advertised, the number rejected, and the number withdrawn from the BGP routing table.
Connections established	Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.
Last reset	Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word “never” is displayed.
Local host:	Displays the peering address of the local router and the TCP port number.
Foreign host:	Displays the peering address of the neighbor and the TCP port number.

Example

```
FTOS#show ip bgp ipv6 unicast neighbors

BGP neighbor is 5ffe:10::3, remote AS 1, external link
  BGP version 4, remote router ID 5.5.5.3
  BGP state ESTABLISHED, in this state for 00:00:32
  Last read 00:00:32, last write 00:00:32
  Hold time is 180, keepalive interval is 60 seconds
  Received 1404 messages, 0 in queue
    3 opens, 1 notifications, 1394 updates
    6 keepalives, 0 route refresh requests
  Sent 48 messages, 0 in queue
    3 opens, 2 notifications, 0 updates
    43 keepalives, 0 route refresh requests
  Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds

  Capabilities received from neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  Capabilities advertised to neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  For address family: IPv6 Unicast
  BGP table version 12, neighbor version 12
  2 accepted prefixes consume 32 bytes

  Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
  Prefixes advertised 0, rejected 0, withdrawn 0 from peer
  Connections established 3; dropped 2
  Last reset 00:00:39, due to Closed by neighbor

  Notification History
    'OPEN error/Bad AS' Sent : 0 Recv: 1

  Local host: 5ffe:10::4, Local port: 179
  Foreign host: 5ffe:10::3, Foreign port: 35470

  Notification History
    'Connection Reset' Sent : 1 Recv: 0

  BGP neighbor is 5ffe:11::3, remote AS 1, external link
    BGP version 4, remote router ID 5.5.5.3
    BGP state ESTABLISHED, in this state for 00:00:28
    Last read 00:00:28, last write 00:00:28
    Hold time is 180, keepalive interval is 60 seconds
    Received 27 messages, 3 notifications, 0 in queue
    Sent 0 messages, 0 notifications, 0 in queue
    Received 8 updates, Sent 0 updates
    Route refresh request: received 0, sent 0
    Minimum time between advertisement runs is 30 seconds
    Minimum time before advertisements start is 0 seconds

  Capabilities received from neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)
    Capabilities advertised to neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  For address family: IPv6 Unicast
  BGP table version 12, neighbor version 12
  2 accepted prefixes consume 32 bytes
  Prefix advertised 0, rejected 0, withdrawn 0

  Connections established 3; dropped 2
  Last reset 00:00:41, due to Closed by neighbor

  Notification History
    'OPEN error/Bad AS' Sent : 0 Recv: 1

Local host: 5ffe:11::4, Local port: 179
```

Related Commands

show ip bgp ipv6 unicast – views the current BGP routing table.

show ip bgp ipv6 unicast peer-group

Allows you to view information on the BGP peers in a peer group.

S5000

Syntax `show ip bgp ipv6 unicast peer-group [peer-group-name [summary]]`

Parameters

peer-group-name	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
summary	(OPTIONAL) Enter the keyword `summary` to view status information of the peers in that peer group. The output is the same as that found in the `show ip bgp ipv6 unicast summary` command.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

neighbor peer-group (assigning peers) – assigns a peer to a peer-group.

neighbor peer-group (creating group) – creates a peer group.

show ip bgp ipv6 unicast summary

Allows you to view the status of all BGP connections.

S5000

Syntax `show ip bgp ipv6 unicast summary`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip bgp ipv6 unicast summary` command shown in the Example below.

Field	Description
BGP router identifier	Displays the local router ID and the AS number.

BGP table version	Displays the BGP table version and the main routing table version.
network entries	Displays the number of network entries, route paths, and the amount of memory used to process those entries.
BGP path attribute entries	Displays the number of BGP path attributes and the amount of memory used to process them.
BGP AS-PATH entries	Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.
BGP community entries	Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The `show ip bgp ipv6 unicast community` command provides more details on the COMMUNITY attributes.
Dampening enabled	Displayed only when dampening is enabled. Displays the number of paths designated as history, dampened, or penalized.
Neighbor	Displays the BGP neighbor address.
AS	Displays the AS number of the neighbor.
MsgRcvd	Displays the number of BGP messages that neighbor received.
MsgSent	Displays the number of BGP messages that neighbor sent.
TblVer	Displays the version of the BGP table that was sent to that neighbor.
InQ	Displays the number of messages from that neighbor waiting to be processed.
OutQ	Displays the number of messages waiting to be sent to that neighbor. If a number appears in parentheses, the number represents the number of messages waiting to be sent to the peer group.
Up/Down	Displays the amount of time (in hours:minutes:seconds) that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word never is displayed.
State/Pfx	If the neighbor is in Established stage, the number of network prefixes received. If a maximum limit was configured with the `neighbor maximum-prefix` command, (prfxd) appears in this column. If the neighbor is not in Established stage, the current stage is displayed (Idle, Connect, Active, OpenSent, OpenConfirm). When the peer is transitioning between states and clearing the routes received, the phrase (Purging) may appear in this column. If the neighbor is disabled, the phrase (Admin shut) appears in this column.

Example

```
FTOS#show ip bgp ipv6 unicast summary
BGP router identifier 5.5.10.4, local AS number 100
BGP table version is 12, main routing table version 12
2 network entrie(s) and 4 paths using 536 bytes of memory
1 BGP path attribute entrie(s) using 112 bytes of memory
1 BGP AS-PATH entrie(s) using 39 bytes of memory
Dampening enabled. 0 history paths, 0 dampened paths, 0
```

```
penalized paths

Neighbor    AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down  State/Pfx

5ffe:10::3  1    28      0       12   0     0 00:01:01   2
5ffe:11::3  1    27      0       12   0     0 00:00:55   2
FTOS#
```

iscsi aging time

Set the aging time for iSCSI sessions.

S5000

Syntax `iscsi aging time` *`time`*

To remove the iSCSI session aging time, use the `no iscsi aging time` command.

Parameters

time	Enter the aging time for the iSCSI session. The range is 5 to 43,200 minutes.

Defaults **10 minutes**

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

27

iSCSI Optimization

Internet small computer system interface (iSCSI) optimization enables quality-of-service (QoS) treatment for iSCSI storage traffic on an S5000 switch.

Use the following Dell Networking operating software (FTOS) commands to configure and verify the iSCSI optimization feature.

advertise dcbx-app-tlv

Configure DCBx to send iSCSI TLV advertisements.

S5000

Syntax

```
advertise dcbx-app-tlv iscsi
```

To disable DCBx iSCSI TLV advertisements, use the `no advertise dcbx-app-tlv iscsi` command.

Defaults Enabled

Command Modes PROTOCOL LLDP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information You can configure iSCSI TLVs to send either globally or on a specified interface. The interface configuration takes priority over global configuration.

iscsi aging time

Set the aging time for iSCSI sessions.

S5000

Syntax

```
iscsi aging time time
```

To remove the iSCSI session aging time, use the `no iscsi aging time` command.

Parameters

time	Enter the aging time for the iSCSI session. The range is 5 to 43,200 minutes.

Defaults 10 minutes

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

iscsi cos

Set the QoS policy that is applied to the iSCSI flows.

S5000

Syntax

```
iscsi cos {enable | disable | dot1p vlan-priority-value
[remark] | dscp dscp-value [remark]}
```

To disable the QoS policy, use the `no iscsi cos dscp` command.

Parameters

enable	Enter the keyword `enable` to allow the application of preferential QoS treatment to iSCSI traffic so that the iSCSI packets are scheduled in the switch with a dot1p priority 4 regardless of the VLAN priority tag in the packet. The default is: the iSCSI packets are handled with dotp1 priority 4 without remark.
disable	Enter the keyword `disable` to disable the application of preferential QoS treatment to iSCSI frames.
dot1p *vlan-priority-value*	Enter the dot1p value of the VLAN priority tag assigned to the incoming packets in an iSCSI session. The range is 0 to 7. The default is the dot1p value in ingress iSCSI frames is not changed and is used in iSCSI TLV advertisements if you did not enter the `iscsi priority-bits` command.
dscp *dscp-value*	Enter the DSCP value assigned to the incoming packets in an iSCSI session. The valid range is 0 to 63. The default is: the DSCP value in ingress packets is not changed.
remark	Marks the incoming iSCSI packets with the configured dot1p or DSCP value when they egress to the switch. The default is: the dot1and DSCP values in egress packets are not changed.

Defaults See Parameters.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information By default, iSCSI flows are assigned to dot1p priority 4. Dell Networking recommends changing the `dot1p priority-queue` setting to 0 (zero).

iscsi enable

Globally enable iSCSI optimization.

S5000

Syntax	`iscsi` *`enable`* To disable iSCSI optimization, use the `no iscsi` command.
Parameters	***enable*** — Enter the keyword `enable` to enable the iSCSI optimization feature.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

iscsi priority-bits

Configure the priority bitmap that advertises in the iSCSI application TLVs.

S5000

Syntax	`iscsi priority-bits` To remove the configured priority bitmap, use the `no iscsi priority-bits` command.
Defaults	4 (0x10 in the bitmap)
Command Modes	PROTOCOL LLDP (only on the global, not on the interface)
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

iscsi profile-compellant

Configure the auto-detection of Dell Compellent arrays on a port.

S5000

Syntax	`iscsi profile-compellent`
Defaults	Dell Compellent disk arrays are not detected.
Command Modes	INTERFACE

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

iscsi target port

Configure the iSCSI target ports and optionally, the IP addresses on which iSCSI communication is monitored.

S5000

Syntax

`iscsi target port [`*`tcp-port-2...tcp-port-16`*`]ip-address [`*`ip-address`*`]`

To remove the configured iSCSI target ports or IP addresses, use the `no iscsi target port` command.

Parameters

tcp-port-2...tcpport-16	Enter the tcp-port number of the iSCSI target ports. The `tcp-port-n` is the TCP port number or a list of TCP port numbers on which the iSCSI target listens to requests. Separate port numbers with a comma. The default is **860, 3260**.
ip-address (Optional)	Enter the ip-address that the iSCSI monitors. The ip-address specifies the IP address of the iSCSI target.

Defaults **860, 3260**

Command Modes CONFIGURATION

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Usage Information

You can configure up to 16 target TCP ports on the switch in one command or multiple commands.

When you use the `no iscsi target port` command and the TCP port to be deleted is one bound to a specific IP address, the IP address value must be included in the command.

show iscsi

Display the currently configured iSCSI settings.

S5000

Syntax `show iscsi`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show iscsi
iSCSI is enabled
iSCSI session monitoring is disabled
iSCSI COS : dot1p is 4 no-remark
Session aging time: 10
Maximum number of connections is 256
------------------------------------------------
iSCSI Targets and TCP Ports:
------------------------------------------------
TCP Port Target IP Address
3260
860
```

Related Commands

- show iscsi session – displays information about active iSCSI sessions on the switch.
- show iscsi session detailed – displays detailed information about active iSCSI sessions on the switch.
- show run iscsi – shows `run iscsi`.

show iscsi session

Display information about active iSCSI sessions on the switch.

S5000

Syntax `show iscsi session`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS# show iscsi session
Session 0:
------------------------------------------------------
Target: iqn.2001-05.com.equallogic:
0-8a0906-0e70c2002-10a0018426a48c94-iom010
Initiator: iqn.1991-05.com.microsoft:win-x9l8v27yajg
ISID: 400001370000

Session 1:
---------------------------------------------------------
Target: iqn.2001-05.com.equallogic:
0-8a0906-0f60c2002-0360018428d48c94-iom011
Initiator: iqn.1991-05.com.microsoft:win-x9l8v27yajg
ISID: 400001370000.
```

Related Commands

- show iscsi – displays the currently configured iSCSI settings.
- show iscsi session detailed – displays detailed information about active iSCSI sessions on the switch.
- show run iscsi – shows `run iscsi`.

show iscsi session detailed

Display detailed information on active iSCSI sessions on the switch.

S5000

Syntax `show iscsi session detailed [session` *`isid`*`]`

Parameters

isid	Enter the session's iSCSi ID to display detailed information about the specified iSCSi session.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS# show iscsi session detailed
Session 0 :
---------------------------------------------------
Target:iqn.2010-11.com.ixia:ixload:iscsi-TG1
Initiator:iqn.2010-11.com.ixia.ixload:initiator-iscsi-2c
Up Time:00:00:01:28(DD:HH:MM:SS)
Time for aging out:00:00:09:34(DD:HH:MM:SS)
ISID:806978696102
Initiator  Initiator Target      Target  Connection
IP Address TCP Port  IP Address  TCPPort ID
10.10.0.44 33345     10.10.0.101 3260    0
Session 1 :
----------------------------------------------------
Target:iqn.2010-11.com.ixia:ixload:iscsi-TG1
Initiator:iqn.2010-11.com.ixia.ixload:initiator-iscsi-35
Up Time:00:00:01:22(DD:HH:MM:SS)
Time for aging out:00:00:09:31(DD:HH:MM:SS)
ISID:806978696102
Initiator  Initiator Target     Target  Connection
IP Address TCP Port  IP Address TCPPort ID
10.10.0.53 33432     10.10.0.101 3260   0
```

Related Commands

- show iscsi – displays the currently configured iSCSI settings.
- show iscsi session – displays information about active iSCSI sessions on the switch.

- show run iscsi – shows `run iscsi`.

show run iscsi

Display all globally configured non-default iSCSI settings in the current FTOS session.

S5000

Syntax	`show run iscsi`
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Related Commands

- show iscsi – displays the currently configured iSCSI settings.
- show iscsi session – displays detailed information about active iSCSI sessions on the switch.
- show iscsi session detailed – displays detailed information on active iSCSI sessions on the switch.

28

Intermediate System to Intermediate System (IS-IS)

The intermediate system to intermediate system (IS-IS) protocol for IPv4 and IPv6 is supported on the S5000 switch.

IS-IS is an interior gateway protocol that uses a shortest-path-first algorithm. IS-IS facilitates the communication between open systems, supporting routers passing both IP and OSI traffic.

A router is considered an intermediate system. Networks are partitioned into manageable routing domains, called areas. Intermediate systems send, receive, and forward packets to other routers within their area (Level 1 and Level 1-2 devices). Only Level 1-2 and Level 2 devices communicate with other areas.

IS-IS protocol standards are listed in the Standard Compliance chapter in the *FTOS Configuration Guide*.

NOTE: The fundamental mechanisms of IS-IS are the same between IPv4 and IPv6. Where there are differences between the two versions, they are identified and clarified in this chapter. Except where identified, the information in this chapter applies to both protocol versions.

adjacency-check

Verify that the "protocols supported" field of the IS-IS neighbor contains matching values to this router.

S5000

Syntax `adjacency-check`

To disable adjacency check, use the `no adjacency-check` command.

Defaults Enabled.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Use this command to perform protocol-support consistency checks on hello packets. The adjacency-check is enabled by default.

advertise

Leak routes between levels (distribute IP prefixes between Level 1 and Level 2 and vice versa).

S5000

Syntax	`advertise {level1-into-level2 | level2-into-level1}` *`prefix-list-name`* To return to the default, use the `no advertise {level1-into-level2 | level2-into-level1}[`*`prefix-list-name`*`]` command.
Parameters	

level1-into-level2	Enter the keywords `level1-into-level2` to advertise Level 1 routes into Level 2 LSPs. This is the default.
level2-into-level1	Enter the keywords `level2-into-level1` to advertise Level 2 inter-area routes into Level 1 LSPs. This is described in RFC 2966.
prefix-list-name	Enter the name of a configured IP prefix list. Routes meeting the criteria of the IP Prefix list are leaked.

Defaults **level1-into-level2** (Level 1 to Level 2 leaking enabled.)

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You cannot disable leaking from one level to another; however, you can regulate the rate flow from one level to another using an IP Prefix list. If you do not configure the IP Prefix list, all routes are leaked.

You can find additional information in IETF RFC 2966, *Domain-wide Prefix Distribution with Two-Level IS-IS*.

area-password

Configure a hash message authentication code (HMAC) password for an area.

S5000

Syntax `area-password [hmac-md5 | `*`encryption-type`*`]` *`password`*

To delete a password, use the `no area-password` command.

Parameters

hmac-md5	(OPTIONAL) Enter the keywords `hmac-md5` to encrypt the password.

encryption-type	(OPTIONAL) Enter `7` to encrypt the password using DES.
password	Enter a 1 to 16-character length alphanumeric string to prevent unauthorized access or incorrect routing information corrupting the link state database. The password is processed as plain text, which only provides limited security.

Defaults Not configured.

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `area-password` command on routers within an area to prevent the link state database from receiving incorrect routing information from unauthorized routers.

The configured password injects into Level 1 LSPs, CSNPs, and PSNPs.

Related Commands

- domain-password – allows you to set the authentication password for a routing domain.
- isis password – allows you to configure an authentication password for an interface.

clear config

Clear IS-IS configurations that display under the *router isis* heading of the `show running-config` command output.

S5000

Syntax `clear config`

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

CAUTION: Use caution when you enter this command. Back up your configuration prior to using this command or your IS-IS configuration will be erased.

Related Commands

copy – use this command to save the current configuration to another location.

clear isis

Restart the IS-IS process. All IS-IS data is cleared.

S5000

Syntax

```
clear isis [tag] {* | database | traffic}
```

Parameters

tag	(Optional) Enter an alphanumeric string to specify the IS-IS routing tag area.
*****	Enter the keyword `*` to clear all IS-IS information and restart the IS-IS process. This command removes IS-IS neighbor information and IS-IS LSP database information and the full SPF calculation is done.
database	Clears IS-IS LSP database information.
traffic	Clears IS-IS counters.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clns host

Define a name-to-network service mapping point (NSAP) that you use with commands that require NSAPs and system IDs.

S5000

Syntax

```
clns host name nsap
```

Parameters

name	Enter an alphanumeric string to identify the name-to-NSAP mapping.
nsap	Enter a specific NSAP address that is associated with the name parameter.

Defaults Not configured.

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Use this command to configure a shortcut name that you can use instead of entering a long string of numbers associated with an NSAP address.

Related Commands hostname dynamic – enables dynamic learning of host names from routers in the domain and allows the routers to advertise the host names in LSPs.

debug isis

Enable debugging for all IS-IS operations.

S5000

Syntax

`debug isis`

To disable debugging of IS-IS, use the `no debug isis` command.

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Entering `debug isis` enables all debugging parameters.

Use this command to display all debugging information in one output. To turn off debugging, you normally enter separate `no` forms of each command. Enter the `no debug isis` command to disable all debug messages for IS-IS at once.

debug isis adj-packets

Enable debugging on adjacency-related activity such as hello packets that are sent and received on IS-IS adjacencies.

S5000

Syntax

`debug isis adj-packets [`*`interface`*`]`

To turn off debugging, use the `no debug isis adj-packets [`*`interface`*`]` command.

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` followed by a number. The range is 1 to 128. • For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug isis local-updates

Enables debugging on a specific interface and provides diagnostic information to debug IS-IS local update packets.

S5000

Syntax

`debug isis local-updates [interface]`

To turn off debugging, use the `no debug isis local-updates [interface]` command.

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` followed by a number. The range is 1 to 128. • For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug isis snp-packets

Enable debugging on a specific interface and provides diagnostic information to debug IS-IS complete sequence number PDU (CSNP) and partial sequence number PDU (PSNP) packets.

S5000

Syntax

`debug isis snp-packets [interface-type slot/port]`

To turn off debugging, use the `no debug isis snp-packets [interface-type slot/port]` command.

Parameters

interface-type slot/port	(OPTIONAL) Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug isis spf-triggers

Enable debugging on the events that triggered IS-IS shortest path first (SPF) events for debugging purposes.

S5000

Syntax `debug isis spf-triggers`

To turn off debugging, use the `no debug isis spf-triggers` command.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug isis update-packets

Enable debugging on link state PDUs (LSPs) that are detected by a router.

S5000

Syntax `debug isis update-packets [interface-type slot/port]`

To turn off debugging, use the `no debug isis update-packets [interface-type slot/port]` command.

Parameters

interface-type slot/port	(OPTIONAL) Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below.

- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

default-information originate

Generates a default route into an IS-IS routing domain and controls the distribution of default information.

S5000

Syntax

`default-information originate [always] [metric` *`metric`*`] [route-map` *`map-name`*`]`

To disable the generation of a default route into the specified IS-IS routing domain, use the `no default-information originate [always] [metric` *`metric`*`] [route-map` *`map-name`*`]` command.

Parameters

always	(OPTIONAL) Enter the keyword `always` to have the default route always advertised.
metric ***metric***	(OPTIONAL) Enter the keyword `metric` followed by a number to assign to the route. The range is 0 to 16777215.
route-map ***map-name***	(OPTIONAL) A default route is generated by the routing process if the route map is satisfied.

Defaults

Not configured.

Command Modes

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you use this command to redistribute routes into a routing domain, the router becomes an autonomous system (AS) boundary router. An AS boundary router does not always generate a default route into a routing domain. The router still requires its own default route before it can generate one.

How a metric value assigned to a default route advertises depends on the `metric-style` command configuration. If the `metric-style` command is set for Narrow mode and the metric value in the `default-information originate` command is set to a number higher than 63, the metric value advertised in the LSPs is 63. If the `metric-style` command is set for Wide mode, the metric value in the `default-information originate` command is advertised.

Related Commands	- redistribute – redistributes routes from one routing domain to another routing domain. - isis metric – configures a metric for an interface. - metric-style – sets the metric style for the router. - show isis database – displays the IS-IS link state database.

description

Enter a description of the IS-IS routing protocol.

S5000

Syntax

`description {*description*}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description to identify the IS-IS protocol (80 characters maximum).

Defaults none

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands router isis – Enter ROUTER mode on the switch.

distance

Define the administrative distance for learned routes.

S5000

Syntax

`distance weight [ip-address mask [prefix-list]]`

To return to the default values, use the `no distance weight` command.

Parameters

weight	The administrative distance value indicates the reliability of a routing information source. The range is 1 to 255. (A higher relative value

	indicates lower reliability. Routes with smaller values are given preference.) The default is **115**.
ip-address mask	(OPTIONAL) Enter an IP address in dotted decimal format and enter a mask in either dotted decimal or /prefix format.
prefix-list	(OPTIONAL) Enter the name of a prefix list name.

Defaults

weight = **115**

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The administrative distance indicates the trust value of incoming packets. A low administrative distance indicates a high trust rate. A high value indicates a lower trust rate. For example, a weight of 255 is interpreted that the routing information source is not trustworthy and should be ignored.

distribute-list in

Filter network prefixes received in updates.

S5000

Syntax

`distribute-list [prefix-list-name] in [interface-type slot/port]`

To return to the default values, use the `no distribute-list prefix-list-name in [interface-type slot/port]` command.

Parameters

prefix-list-name in	Specify the prefix list to filter prefixes in routing updates followed by the keyword `in`.
interface-type slot/port	(OPTIONAL) Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below.

- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults Not configured.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

- distribute-list out – suppresses networks from being advertised in updates.
- redistribute – redistributes routes from one routing domain to another routing domain.

distribute-list out

Suppress network prefixes from being advertised in outbound updates.

S5000

Syntax `distribute-list prefix-list-name out [connected | bgp as number | ospf process-id | rip | static]`

To return to the default values, use the `no distribute-list prefix-list-name out [bgp as number connected | ospf process-id | rip | static]` command.

Parameters

***prefix-list-name* out**	Specify the prefix list to filter prefixes in routing updates followed by the keyword `out`.
connected	(OPTIONAL) Enter the keyword `connected` for directly connected routing processes.
ospf *process-id*	(OPTIONAL) Enter the keyword `ospf` followed by the OSPF process-ID number. The range is 1 to 65535.
bgp *as number*	(OPTIONAL) Enter the BGP followed by the AS Number. The range is 1 to 65535.
rip	(OPTIONAL) Enter the keyword `rip` for RIP routes.
static	(OPTIONAL) Enter the keyword `static` for user-configured routing process.

Defaults Not configured.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	You can assign a name to a routing process so a prefix list IS applied to only the routes derived from the specified routing process.
Related Commands	• distribute-list in – filters the networks received in updates. • redistribute – redistributes routes from one routing domain to another routing domain.

distribute-list redistributed-override

Suppress flapping of routes when the same route is redistributed into IS-IS from multiple routers in the network.

S5000

Syntax

`distribute-list redistributed-override in`

To return to the default, use the `no distribute-list redistributed-override in` command.

Defaults

none

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you execute this command, IS-IS does not download the route to the routing table if the same route was redistributed into IS-IS routing protocol on the same router.

domain-password

Set the authentication password for a routing domain.

S5000

Syntax

`domain-password [hmac-md5 | encryption-type] password`

To disable the password, use the `no domain-password` command.

Parameters

hmac-md5	(OPTIONAL) Enter the keywords `hmac-md5` to encrypt the password using MD5.
encryption-type	(OPTIONAL) Enter `7` to encrypt the password using DES.
password	Enter an alphanumeric string up to 16 characters long. If you do not specify an `encryption type` or `hmac-md5` keywords, the password is processed as plain text which provides limited security.

Defaults No default password.

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The domain password is inserted in Level 2 link state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).

Related Commands

- area-password – configures an IS-IS area authentication password.
- isis priority – configures the authentication password for an interface.

graceful-restart ietf

Enable graceful restart on an IS-IS router.

S5000

Syntax `graceful-restart ietf`

To return to the default, use the `no graceful-restart ietf` command.

Parameters

ietf	Enter `ietf` to enable graceful restart on the IS-IS router.

Defaults Graceful restart disabled.

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Every graceful restart enabled router’s HELLO PDUs includes a restart TLV. This enables the (re)starting as well as the existing ISIS peers to detect the GR capability of the routers on the connected network. A flag in the Restart TLV contains restart request (RR), restart acknowledge (RA) and suppress adjacency advertisement (SA) bit flags.

The ISIS graceful restart-enabled router can co-exist in mixed topologies where some routers are graceful restart-enabled and others are not. For neighbors that are not graceful restart-enabled, the restarting router brings up the adjacency per the usual methods.

graceful-restart interval

Set the graceful restart grace period, the time during that all graceful restart attempts are prevented.

S5000

Syntax `graceful-restart interval minutes`

To return to the default, use the `no graceful-restart interval` command.

Parameters

minutes	Enter the graceful-restart interval minutes. The range is 1 to 20 minutes. The default is **5 minutes**.

Defaults **5 minutes**

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

graceful-restart t1

Set the graceful restart wait time before unacknowledged restart requests are generated. This wait time is the interval before the system sends a restart request (an IIH with RR bit set in Restart TLV) until the CSNP is received from the helping router.

S5000

Syntax `graceful-restart t1 {interval seconds | retry-times value}`

To return to the default, use the `no graceful-restart t1` command.

Parameters

interval	Enter the keyword `interval` to set the wait time. The range is 5 to 120 seconds. The default is **5 seconds**.
retry-times	Enter the keywords `retry-times` to set the number of times the request interval is extended until a CSNP is received from the helping router. The range is 1 to 10 attempts. The default is **1**.

Defaults Refer to Parameters.

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

graceful-restart t2

Configure the wait time for the graceful restart timer T2 that a restarting router uses as the wait time for each database to synchronize.

S5000

Syntax `graceful-restart t2 {level-1 | level-2}` *`seconds`*

To return to the default, use the `no graceful-restart t2` command.

Parameters

level-1, level-2	Enter the keywords `level-1` or `level-2` to identify the database instance type to which the wait interval applies.
seconds	Enter the `gracefule-restart t2` time in seconds. The range is 5 to 120 seconds. The default is **30 seconds**.

Defaults **30 seconds**

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

graceful-restart t3

Configure the overall wait time before graceful restart completes.

S5000

Syntax `graceful-restart t3 {adjacency | manual}` *`seconds`*

To return to the default, use the `no graceful-restart t3` command.

Parameters

adjacency	Enter the keyword `adjacency` so that the restarting router receives the remaining time value from its peer and adjusts its T3 value so if you have configured this option.
manual	Enter the keyword `manual` to specify a time value that the restarting router uses. The range is 50 to 120 seconds. The default is **30 seconds**.

Defaults manual, **30 seconds**

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	The running router sets the remaining time value to the current adjacency hold time. You can override this setting by implementing this command. Override the default restart-wait time by entering the `no graceful-restart restart-wait` command. When you disable `restart-wait`, the current adjacency hold time is used. Set the t3 timer to `adjacency` on the restarting router when implementing this command. The restarting router gets the remaining time value from its peer and adjusts its T3 value so only when you have configured `graceful-restart t3 adjacency`.
Related Commands	graceful-restart restart-wait – enables the graceful restart maximum wait time before a restarting peer comes up.

graceful-restart restart-wait

Enable the graceful restart maximum wait time before a restarting peer comes up.

S5000

Syntax

NOTE: Set the t3 timer to `adjacency` on the restarting router when implementing this command.

`graceful-restart restart-wait` *`seconds`*

To return to the default, use the `no graceful-restart restart-wait` command.

Parameters

seconds	Enter the graceful restart time in seconds. The range is 5 to 300 seconds. The default is **30 seconds**.

Defaults **30 seconds**

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands graceful-restart t3 – configures the overall wait time before graceful restart completes.

hello padding

Use to turn ON or OFF padding for LAN and point-to-point hello PDUs or to selectively turn padding ON or OFF for LAN or point-to-point hello PDUs.

S5000

Syntax

```
hello padding [multi-point | point-to-point]
```

To return to the default, use the `no hello padding [multi-point | point-to-point]` command.

Parameters

multi-point	(OPTIONAL) Enter the keywords `multi-point` to pad only LAN hello PDUs.
point-to-point	(OPTIONAL) Enter the keywords `point-to-point` to pad only point-to-point PDUs.

Defaults Both LAN and point-to-point hello PDUs are padded.

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information IS-IS hellos are padded to the full maximum transmission unit (MTU) size. Padding IS-IS Hellos (IIHS) to the full MTU provides early error detection of large frame transmission problems or mismatched MTUs on adjacent interfaces.

Related Commands isis hello padding – turns ON or OFF hello padding on an interface basis.

hostname dynamic

Enables dynamic learning of hostnames from routers in the domain and allows the routers to advertise the hostname in LSPs.

S5000

Syntax

```
hostname dynamic
```

To disable this command, use the `no hostname dynamic` command.

Defaults Enabled.

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	Use this command to build name-to-systemID mapping tables through the protocol. All `show` commands that display systems also display the hostname.
Related Commands	clns host – defines a name-to-NSAP mapping.

ignore-lsp-errors

Ignore LSPs with bad checksums instead of purging those LSPs.

S5000

Syntax

`ignore-lsp-errors`

To return to the default values, use the `no ignore-lsp-errors` command.

Defaults

In IS-IS, the default deletes LSPs with internal checksum errors (`no ignore-lsp-errors`).

Command Modes

ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

IS-IS normally purges LSPs with an incorrect data link checksum causing the LSP source to regenerate the message. A cycle of purging and regenerating LSPs can occur when a network link continues to deliver accurate LSPs even though there is a link causing data corruption. This process could cause disruption to your system operation.

ip router isis

Configure IS-IS routing processes on an interface and attach an area tag name to the routing process.

S5000

Syntax

`ip router isis [tag]`

To disable IS-IS on an interface, use the `no ip router isis [tag]` command.

Parameters

tag	(OPTIONAL) The tag you specify identifies a specific area routing process. If you do not specify a tag, a null tag is assigned.

Defaults

No processes are configured.

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	Use the `net` command to assign a network entity title to enable IS-IS.
Related Commands	- net – configures an IS-IS network entity title (NET) for the routing process. - router isis – enables the IS-IS routing protocol.

ipv6 router isis

Enable the IPv6 IS-IS routing protocol and specify an IPv6 IS-IS process.

S5000

Syntax

`ipv6 router isis [tag]`

To disable IS-IS routing, use the `no router isis [tag]` command.

Parameters

tag	(OPTIONAL) This is a unique name for a routing process. A null tag is assumed if the tag option is not specified. The tag name must be unique for all IP router processes for a given router.

Defaults

Not configured.

Command Modes

ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Configure a network entity title (the `net` command) to specify the area address and the router system ID.

Enable routing on one or more interfaces to establish adjacencies and establish dynamic routing.

You can configure only one IS-IS routing process to perform Level 2 routing. A `level-1-2` designation performs Level 1 and Level 2 routing at the same time.

Related Commands

- net – configures an IS-IS network entity title (NET) for the routing process.
- is-type – assigns a type for a given area.

isis circuit-type

Configure the adjacency type on interfaces.

S5000

Syntax

```
isis circuit-type {level-1 | level-1-2 | level-2-only}
```

To return to the default values, use the `no isis circuit-type` command.

Parameters

level-1	You can form a Level 1 adjacency if there is at least one common area address between this system and neighbors. You cannot form Level 2 adjacencies on this interface.
level-1-2	You can form a Level 1 and Level 2 adjacencies when the neighbor is also configured as Level-1-2 and there is at least one common area, if not, a Level 2 adjacency is established. This is the default.
level-2-only	You can form a Level 2 adjacencies when other Level 2 or Level 1-2 routers and their interfaces are configured for Level 1-2 or Level 2. Level 1 adjacencies cannot be established on this interface.

Defaults level-1-2

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Because the default establishes Level 1 and Level 2 adjacencies, you do not need to configure this command. Routers in an IS-IS system must be configured as a Level 1-only, Level 1-2, or Level 2-only system.

Only configure interfaces as Level 1 or Level 2 on routers that are between areas (for example, a Level 1-2 router) to prevent the software from sending unused hello packets and wasting bandwidth.

isis csnp-interval

Configure the IS-IS complete sequence number PDU (CSNP) interval on an interface.

S5000

Syntax

```
isis csnp-interval seconds [level-1 | level-2]
```

To return to the default values, use the `no isis csnp-interval [seconds] [level-1 | level-2]` command.

Parameters

seconds	Interval of transmission time between CSNPs on multi-access networks for the designated intermediate system. The range is 0 to 65535. The default is **10**.

level-1	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 1.
level-2	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 2.

Defaults

seconds = **10**; **level-1** (if not otherwise specified)

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The default values of this command are typically satisfactory transmission times for a specific interface on a designated intermediate system. To maintain database synchronization, the designated routers send CSNPs.

You can configure Level 1 and Level 2 CSNP intervals independently.

isis hello-interval

Specify the length of time between hello packets sent.

S5000

Syntax

```
isis hello-interval seconds [level-1 | level-2]
```

To return to the default values, use the `no isis hello-interval [seconds] [level-1 | level-2]` command.

Parameters

seconds	Allows you to set the length of time between hello packet transmissions. The range is 1 to 65535. The default is **10**.
level-1	(OPTIONAL) Select this value to configure the hello interval for Level 1. This value is the default.
level-2	(OPTIONAL) Select this value to configure the hello interval for Level 2.

Defaults

seconds = **10**; **level-1** (if not otherwise specified)

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Hello packets are held for a length of three times the value of the hello interval. Use a high hello interval seconds to conserve bandwidth and CPU usage. Use a low hello interval seconds for faster convergence (but uses more bandwidth and CPU resources).

Related Commands	isis hello-multiplier – specifies the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency as down.

isis hello-multiplier

Specify the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency down.

S5000

Syntax

`isis hello-multiplier multiplier [level-1 | level-2]`

To return to the default values, use the `no isis hello-multiplier [multiplier] [level-1 | level-2]` command.

Parameters

multiplier	Specifies an integer that sets the multiplier for the hello holding time. Never configure a hello-multiplier lower than the default (3). The range is 3 to 1000. The default is **3**.
level-1	(OPTIONAL) Select this value to configure the hello multiplier independently for Level 1 adjacencies. This value is the default.
level-2	(OPTONAL) Select this value to configure the hello multiplier independently for Level 2 adjacencies.

Defaults

multiplier = **3**; **level-1** (if not otherwise specified)

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The holdtime (the product of the hello-multiplier multiplied by the hello-interval) determines how long a neighbor waits for a hello packet before declaring the neighbor is down so routes can be recalculated.

Related Commands

isis hello-interval – specifies the length of time between hello packets.

isis hello padding

Turn ON or OFF padding of hello PDUs from INTERFACE mode.

S5000

Syntax

`isis hello padding`

To return to the default, use the `no isis hello padding` command.

Defaults	Padding of hello PDUs is enabled (ON).
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Hello PDUs are "padded" only when both the global and interface padding options are ON. Turning either one OFF disables padding for the corresponding interface.
Related Commands	hello padding – turns ON or OFF padding for LAN and point-to-point hello PDUs.

isis ipv6 metric

Assign metric to an interface for use with IPv6 information.

S5000

Syntax

`isis ipv6 metric default-metric [level-1 | level-2]`

To return to the default values, use the `no ipv6 isis metric [default-metric] [level-1 | level-2]` command.

Parameters

default-metric	Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. The range is 0 to 16777215. The default is **10**.
level-1	(OPTIONAL) Enter the keywords `level-1` to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing. This value is the default.
level-2	(OPTIONAL) Enter the keywords `level-2` to configure the SPF calculation for Level 2 (inter-area) routing.

Defaults	default-metric = **10**; **level-1** (if not otherwise specified)
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Dell Networking recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

isis metric

Assign a metric to an interface.

S5000

Syntax

`isis metric default-metric [level-1 | level-2]`

To return to the default values, use the `no isis metric [default-metric] [level-1 | level-2]` command.

Parameters

default-metric	Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. The range is 0 to 63 for narrow and transition metric styles and 0 to 16777215 for wide metric styles. The default is **10**.
level-1	(OPTIONAL) Enter the keywords `level-1` to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing. This is the default.
level-2	(OPTIONAL) Enter the keywords `level-2` to configure the SPF calculation for Level 2 (inter-area) routing.

Defaults default-metric = **10**; **level-1** (if not otherwise specified)

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Dell Networking recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

isis network point-to-point

Enable the software to treat a broadcast interface as a point-to-point interface.

S5000

Syntax

`isis network point-to-point`

To disable the feature, use the `no isis network point-to-point` command.

Defaults Not enabled.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

isis password

Configure an authentication password for an interface.

S5000

Syntax

```
isis password [hmac-md5] password [level-1 | level-2]
```

To delete a password, use the `no isis password [password] [level-1 | level-2]` command.

Parameters

encryption-type	(OPTIONAL) Enter `7` to encrypt the password using DES.
hmac-md5	(OPTIONAL) Enter the keywords `hmac-md5` to encrypt the password using MD5.
password	Assign the interface authentication password.
level-1	(OPTIONAL) Independently configures the authentication password for Level 1. The router acts as a station router for Level 1 routing. This is the default.
level-2	(OPTIONAL) Independently configures the authentication password for Level 2. The router acts as an area router for Level 2 routing.

Defaults No default password. **level-1** (if not otherwise specified).

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To protect your network from unauthorized access, use this command to prevent unauthorized routers from forming adjacencies.

You can assign different passwords for different routing levels by using the keywords `level-1` and `level-2`.

The `no` form of this command disables the password for Level 1 or Level 2 routing, using the respective keywords `level-1` or `level-2`.

This password provides limited security as it is processed as plain text.

isis priority

Set the priority of the designated router you select.

S5000

Syntax

```
isis priority value [level-1 | level-2]
```

To return to the default values, use the `no isis priority [value] [level-1 | level-2]` command.

Parameters

value	This value sets the router priority. The higher the value, the higher the priority. The range is 0 to 127. The default is **64**.
level-1	(OPTIONAL) Specify the priority for Level 1. This is the default.
level-2	(OPTIONAL) Specify the priority for Level 2.

Defaults value = **64**; **level-1** (if not otherwise specified).

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can configure priorities independently for Level 1 and Level 2. Priorities determine which router on a LAN is the designated router. Priorities are advertised within hellos. The router with the highest priority becomes the designated intermediate system (DIS).

NOTE: Routers with a priority of 0 cannot be a designated router.

Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If all the routers have priority 0, one with highest MAC address becomes DIS even though its priority is 0.

is-type

Configure IS-IS operating level for a router.

S5000

Syntax `is-type {level-1 | level-1-2 | level-2-only}`

To return to the default values, use the `no is-type` command.

Parameters

level-1	Allows a router to act as a Level 1 router.
level-1-2	Allows a router to act as both a Level 1 and Level 2 router. This is the default.
level-2-only	Allows a router to act as a Level 2 router.

Defaults **level-1-2**

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The IS-IS protocol automatically determines area boundaries and are able to keep Level 1 and Level 2 routing separate. Poorly planned use of this feature may cause configuration errors, such as accidental area partitioning.

If you are configuring only one area in your network, you do not need to run both Level 1 and Level 2 routing algorithms. You can configure the IS type as Level 1.

log-adjacency-changes

Generate a log messages for adjacency state changes.

S5000

Syntax

```
log-adjacency-changes
```

To disable this function, use the `no log-adjacency-changes` command.

Defaults

Adjacency changes are not logged.

Command Modes

ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command allows you to monitor adjacency state changes, which is useful when you monitor large networks. Messages are logged in the system's error message facility.

lsp-gen-interval

Set the minimum interval between successive generations of link-state packets (LSPs).

S5000

Syntax

```
lsp-gen-interval [level-l | level-2] interval seconds
[initial_wait_interval seconds [second_wait_interval seconds]]
```

To restore default values, use the `no lsp-gen-interval [level-l | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]` command.

Parameters

level-l	(OPTIONAL) Enter the keywords `level-1` to apply the configuration to generation of Level-1 LSPs.
level-2	(OPTIONAL) Enter the keywords `level-2` to apply the configuration to generation of Level-2 LSPs.
interval seconds	Enter the maximum number of seconds between LSP generations. The range is 0 to 120 seconds. The default is **5 seconds**.
initial_wait_interval seconds	(OPTIONAL) Enter the initial wait time, in seconds, before running the first LSP generation. The range is 0 to 120 seconds. The default is **1 second**.

second_wait_interval seconds	(OPTIONAL) Enter the wait interval, in seconds, between the first and second LSP generation. The range is 0 to 120 seconds. The default is **5 seconds**.

Defaults Refer to Parameters.

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

LSP throttling slows down the frequency at which LSPs are generated during network instability. Even though throttling LSP generations slows down network convergence, no throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of LSP generations until the topology regains its stability.

The first generation is controlled by the initial wait interval and the second generation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (`interval seconds`). After the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).

lsp-mtu

Set the maximum transmission unit (MTU) of IS-IS link-state packets (LSPs). This command only limits the size of LSPs generated by this router.

S5000

Syntax `lsp-mtu` *`size`*

To return to the default values, use the `no lsp-mtu` command.

Parameters

size	The maximum LSP size, in bytes. The range is 128 to 1497 for Non-Jumbo mode and 128 to 9195 for Jumbo mode. The default is **1497**.

Defaults **1497** bytes.

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The link MTU and the LSP MTU size must be the same.

Because each device can generate a maximum of 255 LSPs, consider carefully whether you should configure the `lsp-mtu` command.

lsp-refresh-interval

Set the link state PDU (LSP) refresh interval. LSPs must be refreshed before they expire. When the LSPs are not refreshed after a refresh interval, they are kept in a database until their `max-lsp-lifetime` reaches zero and then LSPs is purged.

S5000

Syntax

`lsp-refresh-interval *seconds*`

To restore the default refresh interval, use the `no lsp-refresh-interval` command.

Parameters

seconds	The LSP refresh interval, in seconds. This value has to be less than the seconds value specified with the `max-lsp-lifetime` command. The range is 1 to 65535 seconds. The default is **900**.

Defaults

900 seconds

Command Modes

ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The refresh interval determines the rate at which route topology information is transmitted preventing the information from becoming obsolete.

The refresh interval must be less than the LSP lifetime specified with the `max-lsp-lifetime` command. A low value reduces the amount of time that undetected link state database corruption can persist at the cost of increased link utilization. A higher value reduces the link utilization caused by the flooding of refreshed packets.

Related Commands

max-lsp-lifetime – sets the maximum interval that LSPs persist without being refreshed.

max-area-addresses

Configure manual area addresses.

S5000

Syntax

`max-area-addresses *number*`

To return to the default values, use the `no max-area-addresses` command.

Parameters

number	Set the maximum number of manual area addresses. The range is 3 to 6. The default is **3**.

Defaults

3 addresses

Command Modes

ROUTER ISIS

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Usage Information

Use this command to configure the number of area addresses on router. This value must be consistent with routers in the same area, otherwise the router forms only Level 2 adjacencies. The value must be same among all the routers to form Level 1 adjacencies.

max-lsp-lifetime

Set the maximum time that link-state packets (LSPs) exist without being refreshed.

S5000

Syntax

`max-lsp-lifetime seconds`

To restore the default time, use the `no max-lsp-lifetime` command.

Parameters

seconds	The maximum lifetime of LSP in seconds. This value must be greater than the `lsp-refresh-interval` command. The higher the value the longer the LSPs are kept. The range is 1 to 65535. The default is **1200**.

Defaults

1200 seconds

Command Modes

ROUTER ISIS

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Usage Information

Change the maximum LSP lifetime with this command. The maximum LSP lifetime must always be greater than the LSP refresh interval.

The `seconds` parameter enables the router to keep LSPs for the specified length of time. If the value is higher, the overhead is reduced on slower-speed links.

Related Commands

lsp-refresh-interval – use this command to set the link-state packet (LSP) refresh interval.

maximum-paths

Allows you to configure the maximum number of equal cost paths allowed in a routing table.

S5000

Syntax

`maximum-paths number`

To return to the default values, use the `no maximum-paths` command.

Parameters		
	number	Enter a number as the maximum number of parallel paths an IP routing installs in a routing table. The range is 1 to 16. The default is **4**.

Defaults **4**

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

metric-style

Configure a router to generate and accept old-style, new-style, or both styles of type, length, and values (TLV).

S5000

Syntax `metric-style [level-1 | level-2]`

To return to the default values, use the `no metric-style [level-1 | level-2]` command.

Parameters		
	level-1	Enables the metric style on Level 1.
	level-2	Enables the metric style on Level 2.

Command Modes ROUTER ISIS

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you enter the `metric-style wide` command, the FTOS generates and accepts only new-style TLVs. The router uses less memory and other resources rather than generating both old-style and new-style TLVs.

The new-style TLVs have wider metric fields than old-style TLVs.

Related Commands

isis metric – use this command to configure a metric for an interface.

multi-topology

Enables multi-topology IS-IS. It also allows enabling/disabling of old and new style TLVs for IP prefix information in the LSPs.

S5000

Syntax `multi-topology [transition]`

To return to a single topology configuration, use the `no multi-topology [transition]` command.

Parameters

transition	

Defaults Disabled

Command Modes CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6

Command History

Version 9.0(1.3)	Introduced on the S5000.

net

Use this mandatory command to configure an IS-IS network entity title (NET) for a routing process. If you did not configure a NET, the IS-IS process does not start.

S5000

Syntax `net network-entity-title`

To remove a net, use the `no net network-entity-title` command.

Parameters

network-entity-title	Specify the area address and system ID for an IS-IS routing process. The first 1 to 13 bytes identify the area address. The next 6 bytes identify the system ID. The last 1 byte is the selector byte, always identified as zero zero (00). This argument can be applied to an address or a name.

Defaults Not configured.

Command Modes ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

passive-interface

Suppress routing updates on an interface. This command stops the router from sending updates on that interface.

S5000

Syntax	`passive-interface` *`interface-type slot/port`* To delete a passive interface configuration, use the `no passive-interface` *`interface`* command.
Parameters	***interface-type slot/port*** — Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For Loopback interface, enter the keyword `loopback` followed by a number from zero (0) to 16383. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
Defaults	Not configured.
Command Modes	ROUTER ISIS
Command History	**Version 9.0(1.3)** — Introduced on the S5000.
Usage Information	Although the passive interface neither sends nor receives routing updates, the network on that interface is still included in the IS-IS updates sent using other interfaces.

redistribute

Redistribute routes from one routing domain to another routing domain.

S5000

Syntax

`redistribute {static | connected | rip} [level-1 | level-1-2 | level-2] [metric` *`metric-value`*`] [metric-type {external | internal}] [route-map` *`map-name`*`]`

To end redistribution or disable any of the specified keywords, use the `no redistribute {static | connected | rip} [metric` *`metric-value`*`] [metric-type` `{external | internal}] [level-1 | level-1-2 | level-2] [route-map` *`map-name`*`]` command.

Parameters

connected	Enter the keyword `connected` to redistribute active routes into IS-IS.
rip	Enter the keyword `rip` to redistribute RIP routes into IS-IS.
static	Enter the keyword `static` to redistribute user-configured routes into IS-IS.
metric ***metric-value***	(OPTIONAL) Assign a value to the redistributed route. The range is 0 to 16777215. The default is **0**. Use a value that is consistent with the destination protocol.
metric-type {external | internal}	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. Specify one of the following: • `external` • `internal`
level-1	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.
level-1-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level-1-2 routes.
level-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes. This is the default.
route-map ***map-name***	(OPTIONAL) If you do not enter the route-map argument, all routes are redistributed. If a map-name value is not specified, no routers are imported.

Defaults

- metric metric-value = **0**
- metric-type= internal; **level-2**

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To redistribute a default route (0.0.0.0/0), configure the `default-information originate` command.

Changing or disabling a keyword in this command does not affect the state of the other command keywords.

When an LSP with an internal metric is received, the FTOS considers the route cost while considering the advertised cost to reach the destination.

Redistributed routing information is filtered with the `distribute-list out` command to ensure that the routes are properly are passed to the receiving routing protocol.

How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the `metric-style` command. If the `metric-style` command is set for Narrow or Transition mode and the metric value in the `redistribute` command is set to a number higher than 63, the metric value advertised in LSPs is 63. If the `metric-style` command is set for Wide mode, the metric value in the `redistribute` command is advertised.

Related Commands

- default-information originate – generates a default route for the IS-IS domain.
- distribute-list out – suppresses networks from being advertised in updates. This command filters redistributed routing information.

redistribute bgp

Redistribute routing information from a BGP process.

S5000

Syntax

```
redistribute bgp AS number [level-1| level-1-2 | level-2]
[metric metric-value] [metric-type {external| internal}]
[route-map map-name]
```

To return to the default values, use the `no redistribute bgp` command with the appropriate parameters.

Parameters

AS number	Enter a number that corresponds to the autonomous system number. The range is 1 to 65355.
level-1	(OPTIONAL) Routes are independently redistributed into IS-IS Level 1 routes only.
level-1-2	(OPTIONAL) Routes are independently redistributed into IS-IS Level 1 and Level 2 routes.
level-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes only. This is the default.
metric ***metric-value***	(OPTIONAL) The value used for the redistributed route. Use a metric value that is consistent with the destination protocol. The range is 0 to 16777215. The default is **0**.
metric-type {external| internal}	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. The two options are: • `external` • `internal`
route-map ***map-name***	`map-name` is an identifier for a configured route map. The route map filters imported routes from the source routing protocol to the current routing protocol.

If you do not specify a map-name, all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes are imported.

Defaults	**IS-IS Level 2** routes only
Command Modes	- ROUTER ISIS (*for IPv4*) - CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	BGP to IS-IS redistribution supports “match” options using route maps. You can set the metric value, level, and metric-type of redistributed routes by the redistribution command. You can “set” more advanced options using route maps.

Example

```
FTOS(conf)#router is
FTOS(conf-router_isis)#redistribute bgp 1 level-1 metric 32
metric-type
external route-map rmap-isis-to-bgp
FTOS(conf-router_bgp)#show running-config isis
!
router isis
redistribute bgp 1 level-1 metric 32 metric-type external
route-map
rmap-isis-to-bgp
```

redistribute ospf

Redistribute routing information from an OSPF process.

S5000

Syntax

`redistribute ospf` *`process-id`* `[level-1| level-1-2 | level-2] [match {internal | external}] [metric` *`metric-value`*`] [metric-type {external | internal}] [route-map` *`map-name`*`]`

To return to the default values, use the `no redistribute ospf` *`process-id`* `[level-1| level-1-2 | level-2] [match {internal | external}] [metric` *`metric-value`*`][metric-type {external | internal}] [route-map` *`map-name`*`]` command.

Parameters

process-id	Enter a number that corresponds to the OSPF process ID to be redistributed. The range is 1 to 65355.
metric *metric-value*	(OPTIONAL) The value used for the redistributed route. Use a metric value that is consistent with the destination protocol. The range is 0 to 16777215. The default is **0**.

metric-type {external | internal}	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. The two options are: • `external` • `internal`
level-1	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.
level-1-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level-1-2 routes.
level-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes. This is the default.
match {external | internal}	(OPTIONAL) The command used for OSPF to route and redistribute into other routing domains. The values are • `internal` • `external`
route-map *map-name*	`map-name` is an identifier for a configured route map. The route map should filter imported routes from the source routing protocol to the current routing protocol. If you do not specify a map-name, all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes are imported.

Defaults

Refer to Parameters.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the `metric-style` command. If the `metric-style` command is set for Narrow mode and the metric value in the `redistribute ospf` command is set to a number higher than 63, the metric value advertised in LSPs is 63. If the `metric-style` command is set for wide mode, an the metric value in the `redistribute ospf` command is advertised.

router isis

Allows you to enable the IS-IS routing protocol and to specify an IP IS-IS process.

S5000

Syntax

`router isis [tag]`

To disable IS-IS routing, use the `no router isis [tag]` command.

Parameters

tag	(OPTIONAL) This is a unique name for a routing process. A null tag is assumed if the `tag` option is not specified. The tag name must be unique for all IP router processes for a given router.

Defaults

Not configured.

Command Modes

ROUTER ISIS

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must configure a network entity title (the `net` command) to specify the area address and the router system ID.

You must enable routing on one or more interfaces to establish adjacencies and establish dynamic routing.

You can configure only one IS-IS routing process to perform Level 2 routing. A `level-1-2` designation performs Level 1 and Level 2 routing at the same time.

Related Commands

- ip router isis – configures IS-IS routing processes for IP on interfaces and attaches an area designator to the routing process.
- net – configures an IS-IS network entity title (NET) for a routing process.
- is-type – assigns a type for a given area.

set-overload-bit

Configure the router to set the overload bit in its non-pseudonode LSPs. This prevents other routers from using it as an intermediate hop in their shortest path first (SPF) calculations.

S5000

Syntax

`set-overload-bit`

To return to the default values, use the `no set-overload-bit` command.

Defaults

Not set.

Command Modes

- ROUTER ISIS (*for IPv4*)

- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Set the overload bit when a router experiences problems, such as a memory shortage due to an incomplete link state database which can result in an incomplete or inaccurate routing table. If you set the overload bit in its LSPs, other routers ignore the unreliable router in their SPF calculations until the router has recovered.

show config

Display the changes you made to the IS-IS configuration. Default values are not shown.

S5000

Syntax `show config`

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (Router-Isis) The bold section identifies that Multi-Topology IS-IS is enabled in Transition mode.

```
FTOS(conf-router_isis)#show config
!
router isis
clns host ISIS 49.0000.0001.F100.E120.0013.00
log-adjacency-changes
net 49.0000.0001.F100.E120.0013.00
!
address-family ipv6 unicast
maximum-paths 16
multi-topology transition
set-overload-bit
spf-interval level-1 100 15 20
spf-interval level-2 120 20 25
exit-address-family
```

Example (Address-Family_IPv6) The bold section identifies that Multi-Topology IS-IS is enabled in Transition mode.

```
FTOS(conf-router_isis-af_ipv6)#show conf
!
address-family ipv6 unicast
maximum-paths 16
multi-topology transition
set-overload-bit
spf-interval level-1 100 15 20
spf-interval level-2 120 20 25
exit-address-family
```

show isis database

Display the IS-IS link state database.

S5000

Syntax

```
show isis database [level-1 | level-2] [local] [detail |
summary] [lspid]
```

Parameters

level-1	(OPTIONAL) Displays the Level 1 IS-IS link-state database.
level-2	(OPTIONAL) Displays the Level 2 IS-IS link-state database.
local	(OPTIONAL) Displays local link-state database information.
detail	(OPTIONAL) Detailed link-state database information of each LSP displays when specified. If not specified, a summary displays.
summary	(OPTIONAL) Summary of link-state database information displays when specified.
lspid	(OPTIONAL) Display only the specified LSP.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show isis database` command shown in the Example below.

Field	**Description**
IS-IS Level-1/ Level-2 Link State Database	Displays the IS-IS link state database for Level 1 or Level 2.
LSPID	Displays the LSP identifier. The first six octets are the System ID of the originating router. The first six octets are the System ID of the originating router. The next octet is the pseudonode ID. If this byte is not zero, the LSP describes system links. If this byte is zero (0), the LSP describes the state of the originating router. The designated router for a LAN creates and floods a pseudonode LSP and describes the attached systems. The last octet is the LSP number. An LSP will be divided into multiple LSP fragments if there is more data than cannot fit in a single LSP. Each fragment has a unique LSP number. An * after the LSPID indicates that an LSP was originated by the system where this command was issued.

LSP Seq Num	This value is the sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	This is the checksum of the entire LSP packet.
LSP Holdtime	This value is the amount of time, in seconds, that the LSP remains valid. A zero holdtime indicates that this is a purged LSP and is being removed from the link state database. A value between brackets indicates the duration that the purged LSP stays in the database before being removed.
ATT	This value represents the Attach bit. This indicates that the router is a Level 2 router and can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers use the Attach bit to find the closest Level 2 router. They point a default route to the closest Level 2 router.
P	This value represents the P bit. This bit is always set to zero as Dell Networking does not support area partition repair.
OL	This value represents the overload bit, determining congestion. If the overload bit is set, other routers do not use this system as a transit router when calculating routes.

Example

The bold sections identify that Multi-Topology IS-IS is enabled.

```
FTOS#show isis database

IS-IS Level-1 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x00000006 0xCF43    580          0/0/0

IS-IS Level-2 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x00000006 0xCF43    580          0/0/0
!
FTOS#show isis database detail ISIS.00-00

IS-IS Level-1 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x0000002B 0x853B    1075         0/0/0
  Area Address: 49.0000.0001
  NLPID: 0xCC 0x8E
  IP Address: 10.1.1.1
  IPv6 Address: 1011::1
  Topology: IPv4 (0x00) IPv6 (0x8002)
  Metric: 10   IS OSPF.00
  Metric: 10   IS (MT-IPv6) OSPF.00
  Metric: 10   IP 15.1.1.0 255.255.255.0
  Metric: 10   IPv6 (MT-IPv6) 1511::/64
 Metric: 10   IPv6 (MT-IPv6) 2511::/64
 Metric: 10   IPv6 (MT-IPv6) 1011::/64
  Metric: 10   IPv6 1511::/64
  Metric: 10   IP 10.1.1.0 255.255.255.0
    Hostname: ISIS

IS-IS Level-2 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x0000002D 0xB2CD    1075         0/0/0
```

```
  Area Address: 49.0000.0001
  NLPID: 0xCC 0x8E
  IP Address: 10.1.1.1
  IPv6 Address: 1011::1
  Topology: IPv4 (0x00) IPv6 (0x8002)
  Metric: 10   IS OSPF.00
 Metric: 10   IS (MT-IPv6) OSPF.00
  Metric: 10   IP 10.1.1.0 255.255.255.0
  Metric: 10   IP 15.1.1.0 255.255.255.0
  Metric: 20   IP 10.3.3.0 255.255.255.0
  Metric: 10   IPv6 (MT-IPv6) 1011::/64
Metric: 10   IPv6 (MT-IPv6) 1511::/64
Metric: 10   IPv6 (MT-IPv6) 2511::/64
Metric: 20   IPv6 (MT-IPv6) 1033::/64
  Metric: 10   IPv6 2511::/64
  Metric: 20   IPv6 1033::/64
  Hostname: ISIS
FTOS#
```

show isis graceful-restart detail

Display detailed IS-IS graceful restart related settings.

S5000

Syntax

```
show isis graceful-restart detail
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show isis graceful-restart detail
Configured Timer Value
======================
Graceful Restart    : Enabled
T3 Timer            : Manual
T3 Timeout Value    : 30
T2 Timeout Value    : 30 (level-1), 30 (level-2)
T1 Timeout Value    : 5, retry count: 1
Adjacency wait time : 30

Operational Timer Value
======================
Current Mode/State     : Normal/RUNNING
T3 Time left           : 0
T2 Time left           : 0 (level-1), 0 (level-2)
Restart ACK rcv count  : 0 (level-1), 0 (level-2)
Restart Req rcv count  : 0 (level-1), 0 (level-2)
Suppress Adj rcv count : 0 (level-1), 0 (level-2)
Restart CSNP rcv count : 0 (level-1), 0 (level-2)
```

```
Database Sync count    : 0 (level-1), 0 (level-2)
FTOS#
```

show isis hostname

Display IS-IS host names configured or learned on the S5000 switch.

S5000

Syntax `show isis hostname`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show isis hostname
System Id       Dynamic Name Static Name
*F100.E120.0013 Dell         ISIS
FTOS#
```

show isis interface

Display detailed IS-IS interface status and configuration information.

S5000

Syntax `show isis interface [type slot/port]`

Parameters

interface *type slot/port*	(OPTIONAL) Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOSF>show isis int
TenGigabitEthernet 0/7 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 37847070, Local circuit ID 1
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.01
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.01
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 2 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
    LSP Interval: 33
TenGigabitEthernet 0/8 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 38371358, Local circuit ID 2
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.02
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.02
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
--More--
```

show isis neighbors

Display information about neighboring (adjacent) routers.

S5000

Syntax

show isis neighbors [level-1 | level-2] [detail] [*interface-type slot/port*]

Parameters

level-1	(OPTIONAL) Displays information about Level 1 IS-IS neighbors.
level-2	(OPTIONAL) Displays information about Level 2 IS-IS neighbors.
detail	(OPTIONAL) Displays detailed information about neighbors.

interface-type slot/port	(OPTIONAL) Enter one of the following keywords followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use this command to confirm that the neighbor adjacencies are operating correctly. If you suspect that they are not, you can verify the specified area addresses of the routers by using the `show isis neighbors` command.

The following describes the `show isis neighbors` command shown in the Example below.

Field	Description
System Id	The value that identifies a system in an area.
Interface	The interface, slot, and port in which the router was discovered.
State	The value providing status about the adjacency state. The range is Up and Init.
Type	This value displays the adjacency type (Layer 2, Layer 2 or both).
Priority	IS-IS priority advertised by the neighbor. The neighbor with highest priority becomes the designated router for the interface.
Uptime	Displays the interfaces uptime.
Circuit Id	The neighbor's interpretation of the designated router for the interface.

Example

The bold sections below identify that Multi-Topology IS-IS is enabled.

```
FTOS#show isis neighbors
System Id Interface State Type Priority Uptime Circuit Id
TEST Te 7/1 Up L1L2(M) 127 09:28:01 TEST.02
!
FTOS#show isis neighbors detail
System Id Interface State Type Priority Uptime Circuit Id
TEST Te 7/1 Up L1L2(M) 127 09:28:04 TEST.02 Area Address(es):
```

```
49.0000.0001
  IP Address(es): 25.1.1.3*
  MAC Address: 0000.0000.0000
  Hold Time: 28
  Link Local Address: fe80::201:e8ff:fe00:492c
  Topology: IPv4 IPv6 , Common (IPv4 IPv6 )
 Adjacency being used for MTs: IPv4 IPv6
FTOS#
```

show isis protocol

Display IS-IS routing information.

S5000

Syntax `show isis protocol`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

The bold section below identifies that Multi-Topology IS-IS is enabled.

```
FTOS#show isis protocol
IS-IS Router: <Null Tag>
  System Id: F100.E120.0013 IS-Type: level-1-2
  Manual area address(es):
   49.0000.0001
  Routing for area address(es):
   49.0000.0001
  Interfaces supported by IS-IS:
  TenGigabitEthernet 1/0 - IP - IPv6
  TenGigabitEthernet 1/1 - IP - IPv6
  TenGigabitEthernet 1/10 - IP - IPv6
  Loopback 0 - IP - IPv6
Redistributing:
Distance: 115
Generate narrow metrics: level-1-2
Accept narrow metrics:   level-1-2
Generate wide metrics:   none
Accept wide metrics:     none
Multi Topology Routing is enabled in transition mode.
FTOS#
```

show isis traffic

This command allows you to display IS-IS traffic interface information.

S5000

Syntax `show isis traffic [interface-type slot/port]`

Parameters

interface-type slot/port	(OPTIONAL) Enter one of the following keywords followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show isis traffic` command output shown in the Example below.

Table 8. Output Fields for the `show isis traffic` Command

Field	Description
Level-1/Level-2 Hellos (sent/rcvd)	Displays the number. of Hello packets sent and received
PTP Hellos (sent/rcvd)	Displays the number. of point-to-point Hellos sent and received
Level-1/Level-2 LSPs sourced (new/refresh)	Displays the number. of new and refreshed LSPs
Level-1/Level-2 LSPs flooded (sent/rcvd)	Displays the number. of flooded LSPs sent and received

Field	Description
Level-1/Level-2 LSPs CSNPs (sent/ rcvd)	Displays the number. of CSNP LSPs sent and received
Level-1/Level-2 LSPs PSNPs (sent/ rcvd)	Displays the number. of times designated router elections ran
Level-1/Level-2 DR Elections	Displays the number. of times designated router elections ran
Level-1/Level-2 SPF Calculations	Displays the number. of shortest path first calculations
LSP checksum errors received	Displays the number. of checksum errors LSPs received
LSP authentication failures	Displays the number. of LSP authentication failures

Example

```
FTOS#sho is traffic
  IS-IS: Level-1 Hellos (sent/rcvd) : 0/721
  IS-IS: Level-2 Hellos (sent/rcvd) : 900/943
  IS-IS: PTP Hellos (sent/rcvd) : 0/0
  IS-IS: Level-1 LSPs sourced (new/refresh) : 0/0
  IS-IS: Level-2 LSPs sourced (new/refresh) : 1/3
  IS-IS: Level-1 LSPs flooded (sent/rcvd) : 0/0
  IS-IS: Level-2 LSPs flooded (sent/rcvd) : 5934/5217
  IS-IS: Level-1 LSPs CSNPs (sent/rcvd) : 0/0
  IS-IS: Level-2 LSPs CSNPs (sent/rcvd) : 472/238
  IS-IS: Level-1 LSPs PSNPs (sent/rcvd) : 0/0
  IS-IS: Level-2 LSPs PSNPs (sent/rcvd) : 10/337
  IS-IS: Level-1 DR Elections : 4
  IS-IS: Level-2 DR Elections : 4
  IS-IS: Level-1 SPF Calculations : 0
  IS-IS: Level-2 SPF Calculations : 389
  IS-IS: LSP checksum errors received : 0
  IS-IS: LSP authentication failures : 0
FTOS#
```

spf-interval

Specify the minimum interval between shortest path first (SPF) calculations.

S5000

Syntax

`spf-interval [level-l | level-2]` *`interval seconds`* `[`*`initial_wait_interval seconds`* `[`*`second_wait_interval seconds`*`]]`

To restore default values, use the `no spf-interval [level-l | level-2]` *`interval seconds`* `[`*`initial_wait_interval seconds`* `[`*`second_wait_interval seconds`*`]]` command.

Parameters

level-l	(OPTIONAL) Enter the keyword `level-1` to apply the configuration to Level-1 SPF calculations.
level-2	(OPTIONAL) Enter the keyword `level-2` to apply the configuration to Level-2 SPF calculations.
interval seconds	Enter the maximum number of seconds between SPF calculations. The range is 0 to 120 seconds. The default is **10 seconds**.
initial_wait_interval seconds	(OPTIONAL) Enter the initial wait time, in seconds, before running the first SPF calculations. The range is 0 to 120 seconds. The default is **5 seconds**.
second_wait_interval seconds	(OPTIONAL) Enter the wait interval, in seconds, between the first and second SPF calculations. The range is 0 to 120 seconds. The default is **5 seconds**.

Defaults

Refer to Parameters.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command `spf-interval` in CONFIG-ROUTER-ISIS-AF-IPV6 mode is used for IPv6 Multi-Topology route computation only. If using Single Topology mode, use the `spf-interval` command in CONFIG-ROUTER-ISIS mode for both IPv4 and IPv6 route computations.

SPF throttling slows down the frequency at which route calculations are performed during network instability. Even though throttling route calculations slows down network convergence, not throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of route calculations until the topology regains its stability.

The first route calculation is controlled by the initial wait interval and the second calculation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (`interval` `seconds`). After the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).

29

Link Aggregation Control Protocol (LACP)

This chapter contains commands for Dell Networking's implementation of the link aggregation control protocol (LACP) for creating dynamic link aggregation groups (LAGs)—known as "port-channels" in the Dell Networking operating software [FTOS]. The LACP commands in this chapter are supported by FTOS on the S5000 switch.

NOTE: For static LAG commands, refer to Port Channel Commands in the Interfaces chapter), based on the standards specified in the IEEE 802.3 Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

clear lacp counters

Clear Port Channel counters.

S5000

Syntax

```
clear lacp port-channel-number counters
```

Parameters

port-channel-number	Enter a port-channel number: The range is 1 to 128.

Defaults

Without a Port Channel specified, the command clears all Port Channel counters.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

show lacp – displays the lacp configuration.

debug lacp

Debug LACP (configuration, events, etc.)

S5000

Syntax

```
debug lacp [config | events | pdu [interface-type slot/port][in
| out]]
```

To disable LACP debugging, use the `no debug lacp [config | events | pdu [interface-type slot/port][in | out]]` command.

Parameters

config	(OPTIONAL) Enter the keyword `config` to debug the LACP configuration.
events	(OPTIONAL) Enter the keyword `events` to debug the LACP event information.
pdu in | out	(OPTIONAL) Enter the keyword `pdu` to debug the LACP Protocol Data Unit information. Optionally, enter an `in` or `out` parameter to: • Receive enter `in` • Transmit enter `out`
interface-type slot/port	(OPTIONAL) Enter one of the following keywords followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. Optionally, enter an `in` or `out` parameter: • Receive enter `in` • Transmit enter `out`

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

lacp long-timeout

Configure a long timeout period (30 seconds) for an LACP session.

S5000

Syntax

```
lacp long-timeout
```

To reset the timeout period to a short timeout (1 second), use the `no lacp long-timeout` command.

Defaults	**1 second**
Command Modes	INTERFACE (conf-if-po-number)
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	This command applies to dynamic port-channel interfaces only. When applied on a static port-channel, this command has no effect.
Related Commands	show lacp – displays the lacp configuration.

lacp port-priority

Configure the port priority to influence which ports will be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

S5000

Syntax

`lacp port-priority priority-value`

To return to the default setting, use the `no lacp port-priority priority-value` command.

Parameters

priority-value	Enter the port-priority value. The higher the value number, the lower the priority. The range is 1 to 65535. The default is **32768**.

Defaults	**32768**
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

lacp system-priority

Configure the LACP system priority.

S5000

Syntax

`lacp system-priority priority-value`

Parameters

priority-value	Enter the port-priority value. The higher the value number, the lower the priority. The range is 1 to 65535. The default is **32768**.

Defaults **32768**

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

port-channel mode

Configure the LACP port channel mode.

S5000

Syntax `port-channel` *`number`* `mode [active] [passive] [off]`

Parameters

number	Enter the keywords `port-channel` followed by a number. The range is 1 to 128.
active	Enter the keyword `active` to set the mode to the active state. **NOTE:** LACP modes are defined in *Usage Information* below.
passive	Enter the keyword `passive` to set the mode to the passive state. **NOTE:** LACP modes are defined in *Usage Information* below.
off	Enter the keyword `off` to set the mode to the off state. **NOTE:** LACP modes are defined in *Usage Information* below.

Defaults off

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

LACP Modes

active	An interface is in an active negotiating state in this mode. LACP runs on any link configured in the active state and also automatically initiates negotiation with other ports by initiating LACP packets.
passive	An interface is not in an active negotiating state in this mode. LACP runs on any link configured in the passive state. Ports in a passive state respond to negotiation requests from other ports that are in active states. Ports in a passive state respond to LACP packets
off	An interface can not be part of a dynamic port channel in off mode. LACP does not run on a port configured in off mode.

port-channel-protocol lacp

Enable LACP on any LAN port.

S5000

Syntax

`port-channel-protocol lacp`

To disable LACP on a LAN port, use the `no port-channel-protocol lacp` command.

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

show lacp – displays the LACP information.

show interfaces port-channel – displays information on configured Port Channel groups.

show lacp

Display the LACP matrix.

S5000

Syntax

`show lacp port-channel-number [sys-id | counters]`

Parameters

port-channel-number	Enter a port-channel number: The range is 1 to 128.
sys-id	(OPTIONAL) Enter the keywords `sys-id` and the value that identifies a system.
counters	(OPTIONAL) Enter the keyword `counters` to display the LACP counters.

Defaults

Without a Port Channel specified, the command clears all Port Channel counters.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (Port-Channel-Number)

```
FTOS#show lacp 1
Port-channel 1 admin up, oper up, mode lacp
Actor   System ID: Priority 32768, Address 0001.e800.a12b
Partner System ID: Priority 32768, Address 0001.e801.45a5
                   Actor Admin Key 1, Oper Key 1, Partner Oper
Key 1
                   LACP LAG 1 is an aggregatable link
```

```
A - Active LACP, B - Passive LACP, C - Short Timeout, D - Long
Timeout
E - Aggregatable Link, F - Individual Link, G - IN_SYNC, H -
OUT_OF_SYNC
I - Collection enabled, J - Collection disabled, K -
Distribution enabled L - Distribution disabled,
M - Partner Defaulted, N - Partner Non-defaulted, O - Receiver
is in expired state,
P - Receiver is not in expired state

Port Te 10/6 is enabled, LACP is enabled and mode is lacp
  Actor   Admin: State ACEHJLMP Key 1    Priority 128
           Oper: State ACEGIKNP Key 1    Priority 128
  Partner Admin: State BDFHJLMP Key 0    Priority 0
           Oper: State BCEGIKNP Key 1    Priority 128
FTOS#
```

Example (Sys-id)

```
FTOS#show lacp 1 sys-id
Actor    System ID: Priority 32768, Address 0001.e800.a12b
Partner  System ID: Priority 32768, Address 0001.e801.45a5

FTOS#
```

Example (Counter)

```
FTOS#show lacp 1 counters
----------------------------------------------------
           LACP PDU    Marker PDU   Unknown   Illegal
Port     Xmit Recv   Xmit Recv      Pkts Rx   Pkts Rx
-----------------------------------------------------
Te 10/6  200  200     0    0        0          0
FTOS#
```

Related Commands

clear lacp counters – clears the LACP counters.

show interfaces port-channel – displays information on configured Port Channel groups.

30

Layer 2

This chapter describes commands to configure Layer 2 features.

This chapter contains the following sections:

- MAC Addressing Commands
- Virtual LAN (VLAN) Commands
- Far-End Failure Detection (FEFD)

The VLAN commands are supported on the S5000 Dell Networking switch.

MAC Addressing Commands

The following commands are related to configuring, managing, and viewing MAC addresses.

clear mac-address-table dynamic

Clear the MAC address table of all MAC address learned dynamically.

S5000

Syntax

```
clear mac-address-table {dynamic | sticky }{address mac-address
| all | interface type slot/port | vlan vlan-id}
```

Parameters

dynamic	Enter the keyword `dynamic` to specify dynamically-learned MAC addresses.
sticky	Enter the keyword `sticky` to specify sticky MAC addresses.
address *mac-address*	Enter the keyword `address` followed by a MAC address in nn:nn:nn:nn:nn:nn format.
all	Enter the keyword `all` to delete all MAC address entries in the MAC address table.
interface *type slot/port*	Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.

		- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. - For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
	vlan *vlan-id*	Enter the keyword `vlan` followed by a VLAN ID number from 1 to 4094.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

mac-address-table aging-time

Specify an aging time for MAC addresses to be removed from the MAC address table.

S5000

Syntax

```
mac-address-table aging-time seconds
```

Parameters

seconds	Enter either zero (0) or a number as the number of seconds before MAC addresses are relearned. To disable aging of the MAC address table, enter `0`.

Defaults 1800 seconds

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

mac learning-limit – sets the MAC address learning limits for a selected interface.

show mac-address-table aging-time – displays the MAC aging time.

mac-address-table static

Associate specific MAC or hardware addresses to an interface and VLANs.

S5000

Syntax

```
mac-address-table static mac-address output interface-type
slot/port vlan vlan-id
```

To remove a MAC address, use the `no mac-address-table static` *`mac-address`* `output` *`interface-type slot/port`* `vlan` *`vlan-id`* command.

Parameters

mac-address	Enter the 48-bit hexidecimal address in nn:nn:nn:nn:nn:nn format.
output *interface-type slot/port*	Enter the keyword `output` followed by one of the following interfaces: • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
vlan *vlan-id*	Enter the keyword `vlan` followed by a VLAN ID number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands show mac-address-table – displays the MAC address table.

mac-address-table station-move threshold

Change the frequency with which the MAC address station-move trap is sent after a MAC address changes in a VLAN. A trap is sent if a station move is detected above a threshold number of times in a given interval.

S5000

Syntax

```
[no] mac-address-table station-move threshold number interval
count
```

Parameters

threshold *number*	Enter the keyword `threshold` followed by the number of times MAC addresses in VLANs can change before an SNMP trap is sent. The range is 1 to 10.
interval *seconds*	Enter the keyword `interval` followed by the number of seconds. The range is 5 to 60.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information For information about the specific trap sent and the corresponding Syslog, refer to the SNMP Traps chapter.

mac-address-table station-move refresh-arp

Ensure that address resolution protocol (ARP) refreshes the egress interface when a station move occurs due to a topology change.

S5000

Syntax

```
[no] mac-address-table station-move refresh-arp
```

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information For details about using this command, refer to the “NIC Teaming” section of the Layer 2 chapter in the *FTOS Configuration Guide*.

mac learning-limit

Limit the maximum number of MAC addresses (static + dynamic) learned on a selected interface.

S5000

Syntax

```
mac learning-limit [address_limit ] | [learn-limit-violation] |
[station-move-violation]
```

Parameters

address_limit	Enter the maximum number of MAC addresses that can be learned on the interface. The range is 1 to 1000000.
learn-limit-violation	(OPTIONAL) Enter the `learn-limit-violation` keyword to specify an action when the learn limit is reached.
station-move-violation	(OPTIONAL) Enter the keywords `station-move` to specify an action when the station move limit is reached.

Defaults Default behavior is dynamic.

NOTE: “Static” means manually entered addresses, which do not age.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command and its options are supported on physical interfaces, static LAGs, LACP LAGs, and VLANs.

If you do not specify the `vlan` option, the MAC address counters is not VLAN-based. That is, the sum of the addresses learned on all VLANs (not having any learning limit configuration) is counted against the MAC learning limit.

MAC Learning Limit violation logs and actions are not available on a per-VLAN basis.

With the keyword `no-station-move` option, MAC addresses learned through this feature on the selected interface persist on a per-VLAN basis, even if received on another interface. Enabling or disabling this option has no effect on already learned MAC addresses.

After the MAC address learning limit is reached, learned MAC addresses start to age out. To clear statistics on MAC address learning, use the `clear counters` command with the learning-limit parameter.

NOTE: If you configure this command on an interface in a routed VLAN, and after the MAC addresses learned reaches the limit set in the `mac learning-limit` command, IP protocols are affected. For example, VRRP sets multiple VRRP Masters and OSPF may not come up.

When a channel member is added to a port-channel and there is not enough ACL CAM space, the MAC limit functionality on that port-channel is undefined. When this occurs, un-configure the existing configuration first and then reapply the limit with a lower value.

Related Commands

clear counters – Clear counters used in the `show interface` command.

clear mac-address-table dynamic – clears the MAC address table of all MAC address learned dynamically.

mac learning-limit mac-address-sticky – Replaces deprecated `no-station-move` parameter.

show mac learning-limit – displays MAC learning-limit configuration.

mac learning-limit learn-limit-violation

Configure an action for a MAC address learning-limit violation.

S5000

Syntax

```
mac learning-limit learn-limit-violation {log | shutdown}
```

To return to the default, use the `no mac learning-limit learn-limit-violation {log | shutdown}` command.

Parameters

log	Enter the keyword `log` to generate a syslog message on a learning-limit violation.

shutdown	Enter the keyword `shutdown` to shut down the port on a learning-limit violation.

Defaults none

Command Modes INTERFACE (conf-if-interface-slot/port)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This is supported on physical interfaces, static LAGs, and LACP LAGs.

Related Commands show mac learning-limit – displays details of the mac learning-limit.

mac learning-limit mac-address-sticky

Maintain the dynamically-learnt mac addresses as sticky MAC addresses on the selected port.

S5000

Syntax

```
mac learning-limit mac-address-sticky
```

To convert the sticky MAC addresses to dynamic MAC addresses, use the `no mac learning-limit` command.

Parameters

mac-address-sticky	Configures the dynamic MAC addresses as sticky on an interface.

Defaults none

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If you configure `mac-learn-limit` and the sticky MAC feature is enabled, dynamically-learned MAC addresses are converted to sticky for that port. Any new MAC address that is learned also becomes sticky for that port.

Related Commands show mac learning-limit – Displays the details of the mac learning-limit.

mac learning-limit station-move-violation

Specify the actions for a station move violation.

S5000

Syntax

```
mac learning-limit station-move-violation {log | shutdown-both
| shutdown-offending | shutdown-original}
```

To disable a configuration, use the `no mac learning-limit station-move-violation` command, followed by the configured keyword.

Parameters

log	Enter the keyword `log` to generate a syslog message on a station move violation.
shutdown-both	Enter the keyword `shutdown` to shut down both the original and offending interface and generate a syslog message.
shutdown-offending	Enter the keywords `shutdown-offending` to shut down the offending interface and generate a syslog message.
shutdown-original	Enter the keywords `shutdown-original` to shut down the original interface and generate a syslog message.

Defaults none

Command Modes INTERFACE (conf-if-interface-slot/port)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This is supported on physical interfaces, static LAGs, and LACP LAGs.

Related Commands show mac learning-limit – displays details of the mac learning-limit.

mac learning-limit reset

Reset the MAC address learning-limit error-disabled state.

S5000

Syntax `mac learning-limit reset`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

show cam mac stack-unit

Display the content addressable memory (CAM) size and the portions allocated for MAC addresses and for MAC ACLs.

S5000

Syntax

```
show cam mac stack-unit unit-number [port-set port-pipe]
[address [mac-addr]| dynamic | static | [interface type slot/
port] | [vlan vlan-id]
```

Parameters

stack-unit ***unit-number***	(REQUIRED) Enter the keyword `stack-unit` followed by the unit number. The range is 0 to 11.
port-set ***port-pipe***	(REQUIRED) Enter the keywords `port-set` followed by a Port-Pipe number to select the Port-Pipe for which to gather information. The range is 0 or 1.
address ***mac-addr***	(OPTIONAL) Enter the keyword `address` followed by a MAC address in the nn:nn:nn:nn:nn:nn format to display information on that MAC address.
dynamic	(OPTIONAL) Enter the keyword `dynamic` to display only those MAC addresses learned dynamically by the switch.
static	(OPTIONAL) Enter the keyword `static` to display only those MAC address specifically configured on the switch.
interface ***type slot/port***	(OPTIONAL) Enter the keyword `interface` followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
vlan ***vlan-id***	(OPTIONAL) Enter the keyword `vlan` followed by the VLAN ID to display the MAC address assigned to the VLAN. The range is 1 to 4094.

Command Modes

- EXEC

- EXEC Privilege

Example

```
FTOS#show cam mac stack-unit 0 port-set 0
VlanId     Mac Address       Region    Interface
 0      5c:f9:dd:ee:ff:c2   LOCAL_DA    00001
 0      ff:ff:ff:ff:ff:ff   STATIC      00001
 0      00:10:18:ff:ff:ff   STATIC      N/A
FTOS#
```

Command History

Version 9.0(1.3)	Introduced on the S5000.

show mac-address-table

Display the MAC address table.

S5000

Syntax

`show mac-address-table [dynamic | static] [address` *`mac-address`* `| interface` *`type slot/port`* `| vlan` *`vlan-id`*`] [count [vlan` *`vlan-id`* `]]]`

Parameters

dynamic	(OPTIONAL) Enter the keyword `dynamic` to display only those MAC addresses learned dynamically by the switch. Optionally, you can also add one of these combinations: `address/`*`mac-address`*, `interface/`*`interface`*, or `vlan` *`vlan-id`*.
static	(OPTIONAL) Enter the keyword `static` to display only those MAC address specifically configured on the switch. Optionally, you can also add one of these combinations: `address/`*`mac-address`*, `interface/`*`interface`*, or `vlan` *`vlan-id`*.
address ***mac-address***	(OPTIONAL) Enter the keyword `address` followed by a MAC address in the nn:nn:nn:nn:nn:nn format to display information on that MAC address.
interface ***type slot/port***	(OPTIONAL) Enter the keyword `interface` followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

interface *interface-type*	(OPTIONAL) Instead of entering the keyword `interface` followed by the interface type, slot and port information, as above, you can enter the interface type, followed by just a slot number.
vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` followed by the VLAN id number to display the MAC address assigned to the VLAN. The range is 1 to 4094.
count	(OPTIONAL) Enter the keyword `count`, followed optionally, by an interface or VLAN id number, to display total or interface-specific static addresses, dynamic addresses, and MAC addresses in use.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show mac-address-table` command shown in the Example below.

Column Heading	Description
VlanId	Displays the VLAN ID number.
Mac Address	Displays the MAC address in nn:nn:nn:nn:nn:nn format.
Type	Lists whether the MAC address was manually configured (Static), learned dynamically (Dynamic), or associated with a specific port (Sticky).
Interface	Displays the interface type and slot/port information. The following abbreviations describe the interface types: • gi — Gigabit Ethernet followed by a slot/port. • te — 10-Gigabit Ethernet followed by a slot/port. • fo — 40-Gigabit Ethernet followed by a slot/port. • po — Port Channel followed by a number. The range is 1 to 255.
State	Lists if the MAC address is in use (Active) or not in use (Inactive).

Example

```
FTOS#show mac-address-table
VlanId Mac Address       Type   Interface State
999    00:00:00:00:00:19 Sticky  Te 0/1  Active
999    00:00:00:00:00:29 Dynamic Te 0/2  Active
FTOS#
```

Usage Information

The following describes the `show mac-address-table count` command shown in the Example below.

Line beginning with	Description

MAC Entries...	Displays the number of MAC entries learnt per VLAN.
Dynamic Address...	Lists the number of dynamically learned MAC addresses.
Static Address...	Lists the number of user-defined MAC addresses.
Total MAC...	Lists the total number of MAC addresses used by the switch.

Example (Count)

```
FTOS# show mac-address-table count
MAC Entries for all vlans :
Dynamic Address Count :                 110
Static Address (User-defined) Count : 0
Sticky Address Count :                  0
Total Synced Mac from Peer(N):          100
Total MAC Addresses in Use:             110
FTOS#
```

Related Commands

show mac-address-table aging-time – displays MAC aging time.

show mac-address-table aging-time

Display the aging times assigned to the MAC addresses on the switch.

S5000

Syntax

```
show mac-address-table aging-time [vlan vlan-id]
```

Parameters

vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` followed by the VLAN ID to display the MAC address assigned to the VLAN. The range is 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show mac-address-table aging-time
  Mac-address-table aging time : 1800

FTOS#
```

Related Commands

show mac-address-table – displays the current MAC address configuration.

show mac accounting access-list

Display destination counters for Layer 2 traffic (available on physical interfaces only).

S5000

Syntax

```
show mac accounting {access—list name {interface type slot/
port} {in | out}}}
```

Parameters

access-list *name*	Enter the name of a configured access-list, up to 140 characters.
interface *type slot/port*	(OPTIONAL) Enter the keyword `interface` followed by the interface type, slot and port information: • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
in | out	Identify whether the ACL is applied on the ingress or egress side.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

MAC Accounting information can be accessed using SNMP via the Force10 MONITOR MIB. For more information about enabling SNMP, refer to the *FTOS Configuration Guide*.

NOTE: Currently, the Force10 MONITOR MIB does not return the MAC addresses in an increasing order using SNMP. As a workaround, you can use the `-C c` option in `snmpwalk` or `snmpbulkwalk` to access the Force10 MONITOR MIB. For example: % snmpwalk -C c -v 2c -c public 133.33.33.131 enterprise.6027.3.3.3

Example

```
FTOS-1#sh mac accounting access-list WORD interface
tengigabitethernet 0/1 in

Destination         Out Port  VLAN  Packets Bytes

00:44:00:00:00:02   Te  11/0  1000  10000   5120000
00:44:00:00:00:01   Te  11/0  1000  10000   5120000
00:22:00:00:00:00   Te  11/0  1000  10000   5120000
00:44:00:00:00:02   Te  11/0  2000  10000   5120000
00:44:00:00:00:01   Te  11/0  2000  10000   5120000

FTOS-1#
```

Related Commands	show mac accounting access-list – displays the MAC access list configurations and counters (if configured).

show mac learning-limit

Display MAC address learning limits set for various interfaces.

S5000

Syntax

```
show mac learning-limit [violate-action] [detail] [interface
type slot/port ]
```

Parameters

violate-action	(OPTIONALY) Enter the keywords `violate-action` to display the MAC learning limit violation status.
detail	(OPTIONAL) Enter the keyword `detail` to display the MAC learning limit in detail.
interface *type slot/port*	(OPTIONAL) Enter the keyword `interface` followed by interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show mac learning-limit interface ten 1/0
Interface  Learning  Dynamic    Static     Unknown SA
Slot/port  Limit     MAC count  MAC count  Drops
Te 1/0     10        0          0          0
```

Virtual LAN (VLAN) Commands

The following commands configure and monitor virtual LANs (VLANs). VLANs are a virtual interface and use many of the same commands as physical interfaces.

You can configure an IP address and Layer 3 protocols on a VLAN called Inter-VLAN routing. FTP, TFTP, ACLs and SNMP are not supported on a VLAN.

Occasionally, while sending broadcast traffic over multiple Layer 3 VLANs, the VRRP state of a VLAN interface may continually switch between Master and Backup.

NOTE: For more information, refer to VLAN Stacking and VLAN-related commands, such as portmode hybrid in the Interfaces chapter.

description

Add a description about the selected VLAN.

S5000

Syntax

`description` *`description`*

Parameters

description	Enter a text string description to identify the VLAN (80 characters maximum).

Defaults

none

Command Modes

INTERFACE VLAN

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

show vlan – displays the VLAN configuration.

default vlan-id

Specify a VLAN as the Default VLAN.

S5000

Syntax

`default vlan-id` *`vlan-id`*

To remove the default VLAN status from a VLAN and VLAN 1 does not exist, use the `no default vlan-id` *`vlan-id`* syntax.

Parameters

vlan-id	Enter the VLAN ID number of the VLAN to become the new Default VLAN. The range is 1 to 4094. The default is **1**.

Defaults	The Default VLAN is VLAN 1.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	To return VLAN 1 as the Default VLAN, use this command syntax (`default-vlan-id 1`). The Default VLAN contains only untagged interfaces.
Related Commands	interface vlan – configures a VLAN.

default-vlan disable

Disable the default VLAN so that all switchports are placed in the Null VLAN until they are explicitly configured as a member of another VLAN.

S5000

Defaults	Enabled.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	`no default vlan disable` is not listed in the running-configuration, but when the default VLAN is disabled, `default-vlan disable` is listed in the running-configuration.

name

Assign a name to the VLAN.

S5000

Syntax	`name` *`vlan-name`* To remove the name from the VLAN, use the `no name` command.
Parameters	***vlan-name*** Enter up to 32 characters as the name of the VLAN.
Defaults	Not configured.
Command Modes	INTERFACE VLAN
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Usage Information	To display information about a named VLAN, enter the `show vlan` command with the name parameter or the show interfaces description command.
Related Commands	description – assigns a descriptive text string to the interface. interface vlan – configures a VLAN. show vlan – displays the current VLAN configurations on the switch.

show config

Display the current configuration of the selected VLAN.

S5000

Syntax

```
show config
```

Command Modes

INTERFACE VLAN

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-if-vl-100)#show config
!
interface Vlan 100
  no ip address
  no shutdown
FTOS(conf-if-vl-100)#
```

show vlan

Display the current VLAN configurations on the switch.

S5000

Syntax

```
show vlan [brief | id vlan-id | name vlan-name]
```

Parameters

brief	(OPTIONAL) Enter the keyword `brief` to display the following information: • VLAN ID • VLAN name (left blank if none is configured) • Spanning Tree Group ID • MAC address aging time • IP address

id *vlan-id*	(OPTIONAL) Enter the keyword `id` followed by a number from 1 to 4094. Only information on the VLAN specified is displayed.
name *vlan-name*	(OPTIONAL) Enter the keyword `name` followed by the name configured for the VLAN. Only information on the VLAN named is displayed.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show vlan` command shown in the Example below.

Column Heading	Description
(Column 1 — no heading)	• asterisk symbol (*) = Default VLAN • G = GVRP VLAN • P = primary VLAN • C = community VLAN • I = isolated VLAN
NUM	Displays existing VLAN IDs.
Status	Displays the word *Inactive* for inactive VLANs and the word *Active* for active VLANs.
Q	• Displays G for GVRP tagged • M for member of a VLAN-Stack VLAN • T for tagged interface • U (for untagged interface) • x (not capitalized x) for Dot1x untagged • X (capitalized X) for Dot1x tagged
Ports	Displays the type, slot, and port information. • Gi = gigabit ethernet • Te = 10 gigabit ethernet • Fo = 40 gigabit ethernet • Po = port channel

Example

```
FTOS#show vlan

Codes: * - Default VLAN, G - GVRP VLANs, P - Primary, C -
Community, I - Isolated
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack
```

```
    NUM  Status      Description   Q Ports
*   1    Inactive
    2    Active                    U Po1(Te 13/0)
                                   T Po20(Te 13/6), Te 13/25
                                   T Te 13/7
    3    Active T Po20(Te 13/6)
                                   T Te 13/7
                                   U Te 13/1
    4    Active U Po2(Te 13/2)
                                   T Po20(Te 13/6)
                                   T Te 13/7
    5    Active T Po20(Te 13/6)
                                   T Te 13/7
                                   U Te 13/3
    6    Active U Po3(Te 13/4)
                                   T Po20(Te 13/6)
                                   T Te 13/7
    7    Active T Po20(Te 13/6)
                                   T Te 13/7
                                   U Te 13/5
P 100    Active T Po1(Te 0/1)
                                   T Te 0/2
C 101    Inactive T Te 0/3
I 102    Inactive T Te 0/4
FTOS#
```

Example (VLAN ID)

```
FTOS# show vlan id 40

Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack

     NUM  Status Description Q Ports
     40   Active             M Te 13/47

FTOS#show vlan id 41

Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack

     NUM  Status Description Q Ports
     41   Active             T Te 13/47

FTOS#show vlan id 42

Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack

     NUM  Status Description Q Ports
     42   Active             U Te 13/47
FTOS#
```

Example (Brief)

```
FTOS#show vlan br
VLAN  Name  STG  MAC Aging   IP Address
---- -----------------------------------
1           0    1800        unassigned
2           0    1800        2.2.2.2/24
```

```
3           0    1800        3.3.3.2/24
FTOS#
```

Example (Name)

```
FTOSconf)#interface vlan 222
FTOS(conf-if-vl-222)#name test
FTOS(conf-if-vl-222)#do show vlan name test

Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack

     NUM  Status Description  Q Ports
     222  Inactive            U Te 1/22
FTOS(conf-if-vl-222)#
```

Related Commands

vlan-stack compatible – enables the Stackable VLAN feature on the selected VLAN.

interface vlan – configures a VLAN.

tagged

Add a Layer 2 interface to a VLAN as a tagged interface.

S5000

Syntax

`tagged interface-type slot/port`

To remove a tagged interface from a VLAN, use the `no tagged interface-type slot/port` command.

Parameters

interface-type slot/port	Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

Defaults

All interfaces in Layer 2 mode are untagged.

Command Modes

INTERFACE VLAN

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you use the `no tagged` command, the interface is automatically placed in the Default VLAN as an untagged interface unless the interface is a member of another VLAN. If the interface belongs to several VLANs, you must remove it from all VLANs to change it to an untagged interface.

Tagged interfaces can belong to multiple VLANs, while untagged interfaces can only belong to one VLAN at a time.

Related Commands

interface vlan – configures a VLAN.

untagged – specifies which interfaces in a VLAN are untagged.

track ip

Track the Layer 3 operational state of a Layer 3 VLAN, using a subset of the VLAN member interfaces.

S5000

Syntax

`track ip` *`interface-type slot/port`*

To remove the tracking feature from the VLAN, use the `no track ip` *`interface-type slot/port`* command.

Parameters

interface-type slot/port	Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

Defaults

Not configured.

Command Modes

INTERFACE VLAN

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When this command is configured, the VLAN is operationally UP if any of the interfaces specified in the `track ip` command are operationally UP, and the VLAN is operationally DOWN if none of the tracking interfaces are operationally UP.

If the `track ip` command is not configured, the VLAN's Layer 3 operational state depends on all the members of the VLAN.

The Layer 2 state of the VLAN, and hence the Layer 2 traffic, is not affected by the `track ip` command configuration.

Related Commands	interface vlan – configures a VLAN. tagged – specifies which interfaces in a VLAN are tagged.

untagged

Add a Layer 2 interface to a VLAN as an untagged interface.

S5000

Syntax

`untagged interface-type slot/port`

To remove an untagged interface from a VLAN, use the `no untagged interface-type slot/port` command.

Parameters

interface-type slot/port	Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

Defaults

All interfaces in Layer 2 mode are untagged.

Command Modes

INTERFACE VLAN

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Untagged interfaces can only belong to one VLAN.

In the Default VLAN, you cannot use the `no untagged interface` command. To remove an untagged interface from all VLANs, including the Default VLAN, enter INTERFACE mode and use the `no switchport` command.

Related Commands

interface vlan – configures a VLAN.

tagged – specifies which interfaces in a VLAN are tagged.

Far-End Failure Detection (FEFD)

The Dell Networking operating software (FTOS) supports far-end failure detection (FEFD) on the Ethernet interfaces of the S5000 switch.

The FEFD feature detects and reports far-end link failures.

- FEFD is not supported on the Management interface.
- During an stack-unit failover, FEFD is operationally disabled for approximately 8-10 seconds.
- By default, FEFD is disabled.

debug fefd

Enable debugging of FEFD.

S5000

Syntax

`debug fefd {events | packets} [`*`interface-type slot/port`*`]`

To disable debugging of FEFD, use the `no debug fefd {events | packets}` `[`*`interface`*`]` command.

Parameters

events	Enter the keyword `events` to enable debugging of FEFD state changes.
packets	Enter the keyword `packets` to enable debugging of FEFD to view information on packets sent and received.
interface-type slot/port	(OPTIONAL) Enter one of the following keywords and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

- fefd – enables far-end failure detection on an interface.
- fefd reset – enables FEFD globally on the system.

fefd

Enable far-end failure detection on an interface.

S5000

Syntax	`fefd` To disable FEFD on an interface, use the `no fefd` command.
Defaults	Disabled.
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	When you enter `no fefd` for an interface and fefd-global, FEFD is enabled on the interface because the `no fefd` command is not retained in the configuration file. To keep the interface FEFD disabled when the global configuration changes, use the `fefd reset` command.
Related Commands	• fefd disable – disables far-end failure detection on an interface. • fefd reset – enables FEFD globally on the system. • fefd mode – changes FEFD mode on an interface.

fefd disable

Disable FEFD on an interface only. This command overrides the `fefd reset` command for the interface.

S5000

Syntax	`fefd disable` To re-enable FEFD on an interface, use the `no fefd disable` command.
Defaults	Not configured.
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	When you enter `no fefd` for an interface and fefd-global, FEFD is enabled on the interface because the `no fefd` command is not retained in the configuration file. To keep the interface FEFD disabled when the global configuration changes, use the `fefd reset` command.
Related Commands	• fefd reset – enables FEFD globally on the system. • fefd mode – changes FEFD mode on an interface.

fefd-global

Enable FEFD globally on the system.

S5000

Syntax

`fefd-global [mode {normal | aggressive}]`

To disable FEFD globally, use the `no fefd-global [mode {normal | aggressive}]` command.

Parameters

normal	(OPTIONAL) Enter the keywords `mode normal` to change the link state to “unknown” when a far-end failure is detected by the software on that interface. When the interface is placed in “unknown” state, the software brings down the line protocol. The default is **Normal mode**.
aggressive	(OPTIONAL) Enter the keywords `mode aggressive` to change the link state to “error-disabled” when a far-end failure is detected by the software on that interface. When an interface is placed in “error-disabled” state, you must enter the `fefd reset` command to reset the interface state.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you enter only the `fefd-global` syntax, the mode is normal and the default interval is 15 seconds.

If you disable FEFD globally (`no fefd-global`), the system does not remove the FEFD interface configuration.

Related Commands

- fefd – enables far-end failure detection.
- fefd-global interval – configures an interval between FEFD control packets.
- show fefdshow fefd – shows the FEFD command output.

fefd-global interval

Configure an interval between FEFD control packets.

S5000

Syntax

`fefd-global interval` *`seconds`*

To return to the default value, use the `no fefd-global interval` command.

Parameters	*seconds*	Enter a number as the time between FEFD control packets. The range is 3 to 300 seconds. The default is **15 seconds**.

Defaults 15 seconds

Command Modes CONFIGURATION

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Related Commands

- fefd – enables far-end failure detection.
- fefd-global – enables FEFD globally on the system.

fefd interval

Set an interval between control packets.

S5000

Syntax `fefd interval seconds`

To return to the default value, use the `no fefd interval` command.

Parameters	*seconds*	Enter a number as the time between FEFD control packets. The range is 3 to 300 seconds. The default is **15 seconds**.

Defaults 15 seconds

Command Modes INTERFACE

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Related Commands

- fefd – enables far-end failure detection.

fefd mode

Change the FEFD mode on an interface.

S5000

Syntax `fefd mode {normal | aggressive}]`

To return the FEFD mode to the default of normal, use the `no fefd mode` command.

Parameters

normal	(OPTIONAL) Enter the keyword `normal` to change the link state to "unknown" when a far-end failure is detected by the software on that interface. When the interface is placed in "unknown" state, the software brings down the line protocol.
aggressive	(OPTIONAL) Enter the keyword `aggressive` to change the link state to "error-disabled" when a far-end failure is detected by the software on that interface. When an interface is placed in "error-disabled" state, you must enter the `fefd reset` command to reset the interface state.

Defaults normal

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

- fefd – enables far-end failure detection.

fefd reset

Reset all interfaces or a single interface that was in "error-disabled" mode.

S5000

Syntax `fefd reset [`*`interface-type slot/port`*`]`

Parameters

interface-type slot/port	(OPTIONAL) Enter one of the following keywords and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

Defaults Not configured.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

- fefd – enables far-end failure detection.

show fefd

View FEFD status globally or on a specific interface.

S5000

Syntax

```
show fefd [interface-type slot/port]
```

Parameters

interface-type slot/port	(OPTIONAL) Enter one of the following keywords and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show fefd` command shown in the Example below.

Field	**Description**
Interface	Displays the interfaces type and number.
Mode	Displays the mode (aggressive or normal) or NA if the interface contains `fefd reset` in its configuration.
Interval	Displays the interval between FEFD packets.
State	Displays the state of the interface and can be one of the following: • bi-directional (interface is up and connected and ing neighbor's echoes). • err-disabled (only found when the FEFD mode is aggressive and when the interface has not n its neighbor's echoes for 3 times the message interval. To reset an interface in this state, use the `fefd reset` command.) • unknown (only found when FEFD mode is normal. • locally disabled (interface contains the `fefd reset` command in its configuration).

- Admin Shutdown (interface is disabled with the `shutdown` command).

Example

```
FTOS#sh fefd
FEFD is globally 'ON', interval is 10 seconds, mode is
'Aggressive'.

INTERFACE MODE       INTERVAL   STATE
                     (second)
Te 5/0   Aggressive  10         Admin Shutdown
Te 5/1   Aggressive  10         Admin Shutdown
Te 5/2   Aggressive  10         Admin Shutdown
Te 5/3   Aggressive  10         Admin Shutdown
Tei 5/4   Aggressive  10         Admin Shutdown
Te 5/5   Aggressive  10         Admin Shutdown
Te 5/6   Aggressive  10         Admin Shutdown
Te 5/7   Aggressive  10         Admin Shutdown
Te 5/8   Aggressive  10         Admin Shutdown
Te 5/9   Aggressive  10         Admin Shutdown
Te 5/10  NA          NA         Locally disabled
Te 5/11  Aggressive  10         Err-disabled
FTOS#
```

Related Commands

- fefd – enables far-end failure detection.
- fefd disable — disables FEFD on an interface only.
- fefd-global – enables FEFD globally on the system.
- fefd reset – resets all interfaces or a single interface that was in “error-disabled” mode.

31

Link Layer Discovery Protocol (LLDP)

Link layer discovery protocol (LLDP) advertises connectivity and management from the local station to the adjacent stations on an IEEE 802 LAN.

This chapter contains the following sections:

- LLPD Commands
- LLDP-MED Commands

LLDP facilitates multi-vendor interoperability by using standard management tools to discover and make available a physical topology for network management. The Dell Networking operating software (FTOS) implementation of LLDP is based on IEEE standard 801.1ab.

FTOS supports the basic LLDP commands on the S5000 switch.

The starting point for using LLDP is invoking LLDP with the `protocol lldp` command in either CONFIGURATION or INTERFACE mode.

The information distributed by LLDP is stored by its recipients in a standard management information base (MIB). You can access the information by a network management system through a management protocol such as simple network management protocol (SNMP).

LLPD Commands

The following are LLDP commands.

advertise dot1-tlv

Advertise dot1 TLVs (Type, Length, Value).

S5000

Syntax

```
advertise dot1-tlv {port-protocol-vlan-id | port-vlan-id |
vlan-name}
```

To remove advertised dot1-tlv, use the `no advertise dot1-tlv {port-protocol-vlan-id | port-vlan-id | vlan-name}` command.

Parameters

port-protocol-vlan-id	Enter the keywords `port-protocol-vlan-id` to advertise the port protocol VLAN identification TLV.
port-vlan-id	Enter the keywords `port-vlan-id` to advertise the port VLAN identification TLV.

	vlan-name	Enter the keywords `vlan-name` to advertise the vlan-name TLV.

Defaults Disabled.

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

protocol lldp (Configuration) – enables LLDP globally.

debug lldp interface – debugs LLDP.

show lldp neighbors – displays the LLDP neighbors.

show running-config lldp – displays the LLDP running configuration.

advertise dot3-tlv

Advertise dot3 TLVs (Type, Length, Value).

S5000

Syntax

```
advertise dot3-tlv {max-frame-size}
```

To remove advertised dot3-tlv, use the `no advertise dot3-tlv {max-frame-size}` command.

Parameters

max-frame-size	Enter the keywords `max-frame-size` to advertise the dot3 maximum frame size.

Defaults none

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

advertise management-tlv

Advertise management TLVs (Type, Length, Value).

S5000

Syntax

```
advertise management -tlv {system-capabilities | system-description | system-name}
```

To remove advertised management TLVs, use the `no advertise management -tlv {system-capabilities | system-description | system-name}` command.

Parameters		
	system-capabilities	Enter the keywords `system-capabilities` to advertise the system capabilities TLVs.
	system-description	Enter the keywords `system-description` to advertise the system description TLVs.
	system-name	Enter the keywords `system-description` to advertise the system description TLVs.

Defaults none

Command Modes CONFIGURATION (conf-lldp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information All three command options—`system-capabilities`, `system-description`, and `system-name`—can be invoked individually or together, in any sequence.

clear lldp counters

Clear LLDP transmitting and receiving counters for all physical interfaces or a specific physical interface.

S5000

Syntax `clear lldp counters interface` *`type slot/port`*

Parameters

interface *type slot/port*	Enter the `interface` keyword followed by the interface type and slot/port information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear lldp neighbors

Clear LLDP neighbor information for all interfaces or a specific interfaces.

S5000

Syntax

```
clear lldp neighbors {interface type slot/port}
```

Parameters

interface *type slot/port*	Enter the `interface` keyword followed by the interface type and slot/port information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug lldp interface

Enable LLDP debugging to display timer events, neighbor additions or deletions, and other information about incoming and outgoing packets.

S5000

Syntax

```
debug lldp interface {interface type slot/port | all}{events |
packet {brief | detail} {tx | rx | both}}
```

To disable debugging, use the `no debug lldp interface {interface | all} {events} {packet {brief | detail} {tx | rx | both}}` command.

Parameters

interface *type slot/port*	Enter the `interface` keyword followed by interface type and slot/port information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

all	(OPTIONAL) Enter the keyword `all` to display information on all interfaces.
events	(OPTIONAL) Enter the keyword `events` to display major events such as timer events.
packet	(OPTIONAL) Enter the keyword `packet` to display information regarding packets coming in or going out.
brief	(OPTIONAL) Enter the keyword `brief` to display brief packet information.
detail	(OPTIONAL) Enter the keyword `detail` to display detailed packet information.
tx	(OPTIONAL) Enter the keyword `tx` to display transmit only packet information.
rx	(OPTIONAL) Enter the keyword `rx` to display receive only packet information.
both	(OPTIONAL) Enter the keyword `both` to display both receive and transmit packet information.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

disable

Enable or disable LLDP.

S5000

Syntax `disable`

To enable LLDP, use the `no disable` command.

Defaults Enabled, that is no disable.

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

protocol lldp (Configuration) – enables LLDP globally.

debug lldp interface – debugs LLDP.

show lldp neighbors – displays the LLDP neighbors.

show running-config lldp – displays the LLDP running configuration.

hello

Configure the rate at which the LLDP control packets are sent to its peer.

S5000

Syntax

`hello seconds`

To revert to the default, use the `no hello seconds` command.

Parameters

seconds	Enter the rate, in seconds, at which the control packets are sent to its peer. The rate is 5 to 180 seconds. The default is **30 seconds**.

Defaults

30 seconds

Command Modes

CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

mode

Set LLDP to receive or transmit.

S5000

Syntax

`mode {tx | rx}`

To return to the default, use the `no mode {tx | rx}` command.

Parameters

tx	Enter the keyword `tx` to set the mode to transmit.
rx	Enter the keyword `rx` to set the mode to receive.

Defaults

Both **transmit** and **receive**.

Command Modes

CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

protocol lldp (Configuration) – enables LLDP globally.

show lldp neighbors – displays the LLDP neighbors.

multiplier

Set the number of consecutive misses before LLDP declares the interface dead.

S5000

Syntax `multiplier` *`integer`*

To return to the default, use the `no multiplier` *`integer`* command.

Parameters

integer	Enter the number of consecutive misses before the LLDP declares the interface dead. The range is 2 to 10.

Defaults **4 x hello**

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

protocol lldp (Configuration)

Enable the LLDP globally on the switch.

S5000

Syntax `protocol lldp`

To disable LLDP globally on the chassis, use the `no protocol lldp` command.

Defaults Disabled.

Command Modes CONFIGURATION (conf-lldp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

protocol lldp (Interface)

Enter the LLDP protocol in INTERFACE mode.

S5000

Syntax `[no] protocol lldp`

To return to the global LLDP configuration mode, use the `no protocol lldp` command from Interface mode.

Defaults	LLDP is not enabled on the interface.
Command Modes	INTERFACE (conf-if-*interface*-lldp)
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Usage Information

Before LLDP can be configured on an interface, it must be enabled globally from CONFIGURATION mode. This command places you in LLDP mode on the interface; it does not enable the protocol.

When you enter the `LLDP` protocol in the Interface context, it overrides global configurations. When you execute the `no protocol lldp` from INTERFACE mode, interfaces begin to inherit the configuration from global LLDP CONFIGURATION mode.

show lldp neighbors

Display LLDP neighbor information for all interfaces or a specified interface.

S5000

Syntax `show lldp neighbors [interface`*`type slot/port`*`] [detail]`

Parameters

interface*type slot/port*	(OPTIONAL) Enter the`interface` keyword followed by interface type and slot/port information: • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
detail	(OPTIONAL) Enter the keyword `detail` to display all the TLV information, timers, and LLDP tx and rx counters.

Defaults	none
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Omitting the keyword `detail` displays only the remote chassis ID, Port ID, and Dead Interval.

Example

```
R1(conf-if-te-1/31)#do show lldp neighbors
Loc PortID Rem  Host Name      Rem     Port Id Rem Chassis Id
-------------------------------------------------------------
```

```
Te 1/21    R2  TenGigabitEthernet  2/11   00:01:e8:06:95:3e
Te 1/31    R3  TenGigabitEthernet  3/11   00:01:e8:09:c2:4a
```

show lldp statistics

Display the LLDP statistical information.

S5000

Syntax `show lldp statistics`

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show lldp statistics
Total number of neighbors: 300
Last table change time    :   Mon Oct 02 16:00:52 2006
Number of Table Inserts  :   1621
Number of Table Deletes  :   200
Number of Table Drops    :   0
Number of Table Age Outs :   400
FTOS#
```

show running-config lldp

Display the current global LLDP configuration.

S5000

Syntax `show running-config lldp`

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show running-config lldp
!
protocol lldp
  advertise dot1-tlv port-protocol-vlan-id port-vlan-id
  advertise dot3-tlv max-frame-size
  advertise management-tlv system-capabilities system-
description
  hello 15
  multiplier 3
  no disable
FTOS#
```

LLDP-MED Commands

The following are the LLDP-MED (Media Endpoint Discovery) commands.

FTOS LLDP-MED commands are an extension of the set of LLDP TLV advertisement commands. The S5000 switch supports all commands.

As defined by ANSI/TIA-1057, LLDP-MED provides organizationally specific TLVs (Type Length Value), so that endpoint devices and network connectivity devices can advertise their characteristics and configuration information. The Organizational Unique Identifier (OUI) for the Telecommunications Industry Association (TIA) is 00-12-BB.

- LLDP-MED Endpoint Device — any device that is on an IEEE 802 LAN network edge, can communicate using IP, and uses the LLDP-MED framework.
- LLDP-MED Network Connectivity Device — any device that provides access to an IEEE 802 LAN to an LLDP-MED endpoint device, and supports IEEE 802.1AB (LLDP) and TIA-1057 (LLDP-MED). The Dell Networking system is an LLDP-MED network connectivity device.

With regard to connected endpoint devices, LLDP-MED provides network connectivity devices with the ability to:

- manage inventory
- manage Power over Ethernet (POE)
- identify physical location
- identify network policy

advertise med guest-voice

Configure the system to advertise a separate limited voice service for a guest user with their own IP telephony handset or other appliances that support interactive voice services.

S5000

Syntax

`advertise med guest-voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}`

To return to the default, use the `no advertise med guest-voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is 1 to 4094.
layer2_priority	Enter the Layer 2 priority. The range is 0 to 7.
DSCP_value	Enter the DSCP value. The range is 0 to 63.
priority-tagged *number*	Enter the keywords `priority-tagged` followed the Layer 2 priority. The range is 0 to 7.

Defaults	Unconfigured.
Command Modes	CONFIGURATION (conf-lldp)
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	protocol lldp (Configuration) – enables LLDP globally. debug lldp interface – debugs LLDP. show lldp neighbors – displays the LLDP neighbors. show running-config lldp – displays the LLDP running configuration.

advertise med guest-voice-signaling

Configure the system to advertise a separate limited voice service for a guest user when the guest voice control packets use a separate network policy than the voice data.

S5000

Syntax

`advertise med guest-voice-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}`

To return to the default, use the `no advertise med guest-voice-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is 1 to 4094.
layer2_priority	Enter the Layer 2 priority. The range is 0 to 7.
DSCP_value	Enter the DSCP value. The range is 0 to 63.
priority-tagged *number*	Enter the keywords `priority-tagged` followed the Layer 2 priority. The range is 0 to 7.

Defaults	unconfigured.
Command Modes	CONFIGURATION (conf-lldp)
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	debug lldp interface – debugs LLDP. show lldp neighbors – displays the LLDP neighbors. show running-config lldp – displays the LLDP running configuration.

advertise med location-identification

Configure the system to advertise a location identifier.

S5000

Syntax

`advertise med location-identification {coordinate-based value | civic-based value | ecs-elin value}`

To return to the default, use the `no advertise med location-identification {coordinate-based value | civic-based value | ecs-elin value}` command.

Parameters

coordinate-based *value*	Enter the keywords `coordinate-based` followed by the coordinated based location in hexadecimal value of 16 bytes.
civic-based *value*	Enter the keywords `civic-based` followed by the civic based location in hexadecimal format. The range is 6 to 255 bytes.
ecs-elin *value*	Enter the keywords `ecs-elin` followed by the Emergency Call Service (ecs) Emergency Location Identification Number (elin) numeric location string. The range is 10 to 25 characters.

Defaults

unconfigured.

Command Modes

CONFIGURATION (conf-lldp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

- ECS — Emergency call service such as defined by TIA or the national emergency numbering association (NENA)
- ELIN — Emergency location identification number, a valid North America Numbering Plan format telephone number supplied for ECS purposes.

Related Commands

debug lldp interface – debugs LLDP.

show lldp neighbors – displays the LLDP neighbors.

show running-config lldp – displays the LLDP running configuration.

advertise med power-via-mdi

Configure the system to advertise the Extended Power via MDI TLV.

S5000

Syntax

`advertise med power-via-mdi`

To return to the default, use the `no advertise med power-via-mdi` command.

Defaults	unconfigured.
Command Modes	CONFIGURATION (conf-lldp)
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Advertise the Extended Power via MDI on all ports that are connected to an 802.3af powered, LLDP-MED endpoint device.
Related Commands	debug lldp interface – debugs LLDP. show lldp neighbors – displays the LLDP neighbors. show running-config lldp – displays the LLDP running configuration.

advertise med softphone-voice

Configure the system to advertise softphone to enable IP telephony on a computer so that the computer can be used as a phone.

S5000

Syntax

`advertise med softphone-voice {vlan-id} | {priority-tagged number}`

To return to the default, use the `no advertise med softphone-voice {vlan-id } | priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is 1 to 4094.
priority-tagged *number*	Enter the keywords `priority-tagged` followed the Layer 2 priority. The range is 0 to 7.

Defaults	unconfigured.
Command Modes	CONFIGURATION (conf-lldp)
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	debug lldp interface – debugs LLDP. show lldp neighbors – displays the LLDP neighbors. show running-config lldp – displays the LLDP running configuration.

advertise med streaming-video

Configure the system to advertise streaming video services for broadcast or multicast-based video. This does not include video applications that rely on TCP buffering.

S5000

Syntax

`advertise med streaming-video {vlan-id} | {priority-tagged number}`

To return to the default, use the `no advertise med streaming-video {vlan-id} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is 1 to 4094.
priority-tagged *number*	Enter the keywords `priority-tagged` followed the Layer 2 priority. The range is 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

debug lldp interface – debugs LLDP.

show lldp neighbors – displays the LLDP neighbors.

show running-config lldp – displays the LLDP running configuration.

advertise med video-conferencing

Configure the system to advertise dedicated video conferencing and other similar appliances that support real-time interactive video

S5000

Syntax

`advertise med video-conferencing {vlan-id} | {priority-tagged number}`

To return to the default, use the `no advertise med video-conferencing {vlan-id} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is 1 to 4094.
priority-tagged *number*	Enter the keywords `priority-tagged` followed the Layer 2 priority. The range is 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

debug lldp interface – debugs LLDP.

show lldp neighbors – displays the LLDP neighbors.

show running-config lldp – displays the LLDP running configuration.

advertise med video-signaling

Configure the system to advertise video control packets that use a separate network policy than video data.

S5000

Syntax `advertise med video-signaling {vlan-id} | {priority-tagged number}`

To return to the default, use the `no advertise med video-signaling {vlan-id} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is 1 to 4094.
priority-tagged *number*	Enter the keywords `priority-tagged` followed the Layer 2 priority. The range is 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

debug lldp interface – debugs LLDP.

show lldp neighbors – displays the LLDP neighbors.

show running-config lldp – displays the LLDP running configuration.

advertise med voice

Configure the system to advertise a dedicated IP telephony handset or other appliances supporting interactive voice services.

S5000

Syntax `advertise med voice {vlan-id} | {priority-tagged number}`

To return to the default, use the `no advertise med voice {vlan-id} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is 1 to 4094.
priority-tagged *number*	Enter the keywords `priority-tagged` followed the Layer 2 priority. The range is 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

debug lldp interface – debugs LLDP.

show lldp neighbors – displays the LLDP neighbors.

show running-config lldp – displays the LLDP running configuration.

advertise med voice-signaling

Configure the system to advertise when voice control packets use a separate network policy than voice data.

S5000

Syntax

```
advertise med voice-signaling {vlan-id} | {priority-tagged
number}
```

To return to the default, use the `no advertise med voice-signaling {vlan-id} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is 1 to 4094.
priority-tagged *number*	Enter the keywords `priority-tagged` followed the Layer 2 priority. The range is 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

debug lldp interface – debugs LLDP.

show lldp neighbors – displays the LLDP neighbors.

show running-config lldp – displays the LLDP running configuration.

32

Multicast Source Discovery Protocol (MSDP)

Multicast source discovery protocol (MSDP) connects multiple PIM Sparse-Mode (PIM-SM) domains together.

MSDP peers connect using TCP port 639. Peers send keepalives every 60 seconds. A peer connection is reset after 75 seconds if no MSDP packets are received. MSDP connections are parallel with MBGP connections.

FTOS supports MSDP commands on the S5000 switch.

debug ip msdp

Turn on MSDP debugging.

S5000

Syntax `debug ip msdp {event peer address | packet peer address | pim}`

To turn debugging off, use the `no debug ip msdp {event peer address | packet peer address | pim}` command.

Parameters

event *peer address*	Enter the keyword `event` followed by the peer address in a dotted decimal format (A.B.C.D.).
packet *peer address*	Enter the keyword `packet` followed by the peer address in a dotted decimal format (A.B.C.D.).
pim	Enter the keyword `pim` to debug advertisement from PIM.

Defaults Not configured.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip msdp cache-rejected-sa

Enable a MSDP cache for the rejected source-active entries.

S5000

Syntax `ip msdp cache-rejected-sa {number}`

To clear the MSDP rejected source-active entries, use the `no ip msdp cache-rejected-sa {number}` command followed by the `ip msdp cache-rejected-sa {number}` command.

Parameters

number	Enter the number of rejected SA entries to cache. The range is 0 to 32766.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands show ip msdp sa-cache rejected-sa

ip msdp default-peer

Define a default peer from which to accept all source-active (SA) messages.

S5000

Syntax `ip msdp default-peer peer address [list name]`

To remove the default peer, use the `no ip msdp default-peer {peer address} list name` command.

Parameters

peer address	Enter the peer address in a dotted decimal format (A.B.C.D.)
list *name*	Enter the keywords `list name` and specify a standard access list that contains the RP address that should be treated as the default peer. If no access list is specified, then all SAs from the peer are accepted.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If a list is not specified, all SA messages received from the default peer are accepted. You can enter multiple `default peer` commands.

ip msdp log-adjacency-changes

Enable logging of MSDP adjacency changes.

S5000

Syntax	`ip msdp log-adjacency-changes` To disable logging, use the `no ip msdp log-adjacency-changes` command.
Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ip msdp mesh-group

Configure a peer to be a member of a mesh group.

S5000

Syntax	`ip msdp mesh-group {`*`name`*`} {`*`peer address`*`}` To remove the peer from a mesh group, use the `no ip msdp mesh-group {`*`name`*`} {`*`peer address`*`}` command.
Parameters	***name*** Enter a string of up to 16 characters long for as the mesh group name. ***peer address*** Enter the peer address in a dotted decimal format (A.B.C.D.).
Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	A MSDP mesh group is a mechanism for reducing SA flooding, typically in an intra-domain setting. When some subset of a domain's MSDP speakers are fully meshed, they can be configured into a mesh-group. If member X of a mesh-group receives a SA message from an MSDP peer that is also a member of the mesh-group, member X accepts the SA message and forwards it to all of its peers that are not part of the mesh-group. However, member X can not forward the SA message to other members of the mesh-group.

ip msdp originator-id

Configure the MSDP Originator ID.

S5000

Syntax

`ip msdp originator-id {`*`interface-type slot/port`*`}`

To remove the originator-id, use the `no ip msdp originator-id {`*`interface-type slot/port`*`}` command.

Parameters

interface-type slot/port	Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip msdp peer

Configure an MSDP peer.

S5000

Syntax

`ip msdp peer `*`peer address`*` [connect-source] [description] [sa-limit `*`number`*`]`

To remove the MSDP peer, use the `no ip msdp peer `*`peer address`*` [connect-source interface] [description `*`name`*`] [sa-limit `*`number`*`]` command.

Parameters

peer address	Enter the peer address in a dotted decimal format (A.B.C.D.).

connect-source *interface*	Enter the keywords `connect-source` followed by one of the interfaces and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` followed by a number. The range is 1 to 128. • For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.
description name	(OPTIONAL) Enter the keyword *description* followed by a description name (maximum 80 characters) to designate a description for the MSDP peer.
sa-limit *number*	(OPTIONAL) Enter the maximum number of SA entries in SA-cache. The range is 1 to 500000. The default it **500000**.

Defaults

as above

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `connect-source` option is used to supply a source IP address for the TCP connection. When an interface is specified using the `connect-source` option, the primary configured address on the interface is used.

If the total number of SA messages received from the peer is already larger than the limit when this command is applied, those SA messages continue to be accepted. To enforce the limit in such situation, use the `clear ip msdp peer` command to reset the peer.

Related Commands

ip msdp sa-limit – configures the MSDP SA Limit.

clear ip msdp peer – clears the MSDP peer.

show ip msdp – displays the MSDP information.

ip msdp redistribute

Filter local PIM SA entries in the SA cache. SAs which are denied by the ACL will time out and not be refreshed. Until they time out, they continue to reside in the MSDP SA cache.

S5000

Syntax	`ip msdp redistribute [list` *`acl-name`*`]`
Parameters	**list** ***acl-name*** — lEnter the name of an extended ACL that contains permitted SAs. If you do not use this option, all local entries are blocked.
Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** — Introduced on the S5000.
Usage Information	Modifications to the ACL do not have an immediate affect on the sa-cache. To apply the redistribute filter to entries already present in the SA cache, use the `clear ip msdp sa-cache local` command.

ip msdp sa-filter

Permit or deny MSDP source active (SA) messages based on multicast source and/or group from the specified peer.

S5000

Syntax	`ip msdp sa-filter {in	out}` *`peer-address`* `list [access-`*`list name`*`]` Remove this configuration using the `no ip msdp sa-filter {in	out}` *`peer address`* `list [access-`*`list name`*`]` command.
Parameters	**in** — Enter the keyword `in` to enable incoming SA filtering. **out** — Enter the keyword `out` to enable outgoing SA filtering. ***peer-address*** — Enter the peer address of the MSDP peer in a dotted decimal format (A.B.C.D.). ***access-list name*** — Enter the name of an extended ACL that contains permitted SAs. If you do not use this option, all local entries are blocked.
Defaults	Not configured.
Command Modes	CONFIGURATION

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

ip msdp sa-limit

Configure the upper limit of source-active (SA) entries in SA-cache.

S5000

Syntax `ip msdp sa-limit number`

To return to the default, use the `no ip msdp sa-limit number` command.

Parameters

number	Enter the maximum number of SA entries in SA-cache. The range is 0 to 40000.

Defaults **50000**

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

FTOS counts the SA messages originated by itself and those received from the MSDP peers. When the total SA messages reach this limit, the subsequent SA messages are dropped (even if they pass RPF checking and policy checking).

If the total number of SA messages is already larger than the limit when this command is applied, those SA messages that are already in FTOS continue to be accepted. To enforce the limit in such situation, use the `clear ip msdp sa-cache` command.

Related Commands

ip msdp peer – configures the MSDP peer.

clear ip msdp peer – clears the MSDP peer.

show ip msdp – displays the MSDP information

ip msdp shutdown

Administratively shut down a configured MSDP peer.

S5000

Syntax `ip msdp shutdown {peer address}`

Parameters

peer address	Enter the peer address in a dotted decimal format (A.B.C.D.).

Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	**Version 9.0(1.3)**	Introduced on the S5000.

ip multicast-msdp

Enable MSDP.

S5000

Syntax

```
ip multicast-msdp
```

To exit MSDP, use the `no ip multicast-msdp` command.

Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	**Version 9.0(1.3)**	Introduced on the S5000.

show ip msdp

Display the MSDP peer status, SA cache, or peer summary.

S5000

Syntax

```
show ip msdp {peer peer address | sa-cache | summary}
```

Parameters

peer *peer address*	Enter the keyword `peer` followed by the peer address in a dotted decimal format (A.B.C.D.).
sa-cache	Enter the keywords `sa-cache` to display the Source-Active cache.
summary	Enter the keyword `summary` to display a MSDP peer summary.

Defaults Not configured.

Command Modes

- EXEC
- EXEC Privilege

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Example

```
FTOS#show ip msdp peer 100.1.1.1

Peer Addr: 100.1.1.1
  Local Addr: 100.1.1.2(639) Connect Source: none
  State: Established Up/Down Time: 00:00:08
  Timers: KeepAlive 60 sec, Hold time 75 sec
  SourceActive packet count (in/out): 0/0
  SAs learned from this peer: 0
  SA Filtering:
  Input (S,G) filter: none
  Output (S,G) filter: none
FTOS#
```

Example (Sa-cache)

```
FTOS#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
GroupAddr  SourceAddr     RPAddr        LearnedFrom Expire
UpTime
224.1.1.1  172.21.220.10  172.21.3.254  172.21.3.254 102
00:02:52
FTOS#
```

Example (Summary)

```
FTOS#show ip msdp summary
Peer Addr  Local Addr State      Source SA  Up/Down Description
72.30.1.2  72.30.1.1  Established  none 0  00:00:03 peer1
72.30.2.2  72.30.2.1  Established  none 0  00:00:03 peer2
72.30.3.2  72.30.3.1  Established  none 0  00:00:02 test-peer-3
FTOS#
```

33

Multiple Spanning Tree Protocol (MSTP)

Multiple spanning tree protocol (MSTP), as implemented by FTOS, conforms to IEEE 802.1s.

MSTP is supported by the Dell Networking operating software (FTOS) on the S5000 switch.

debug spanning-tree mstp

Enable debugging of the multiple spanning tree protocol and view information on the protocol.

S5000

Syntax

```
debug spanning-tree mstp [all | bpdu interface-type slot/port
{in | out} | events]
```

Parameters

all	(OPTIONAL) Enter the keyword all to debug `all` spanning tree operations.
bpdu ***interface-type slot/port*** **{in | out}**	(OPTIONAL) Enter the keyword `bpdu` to debug bridge protocol data units (BPDU). (OPTIONAL) Enter one of the following keywords and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. Optionally, enter an `in` or `out` parameter in conjunction with the optional interface: • For Receive, enter the keyword `in`. • For Transmit, enter the keyword `out`.
events	(OPTIONAL) Enter the keyword `events` to debug MSTP events.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#debug spanning-tree mstp bpdu tengigabitethernet 2/0 ?
in Receive (in)
out Transmit (out)
```

description

Enter a description of the multiple spanning tree.

S5000

Syntax `description {description}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description to identify the multiple spanning tree (maximum 80 characters).

Defaults none

Command Modes SPANNING TREE (The prompt is “config-mstp”.)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands protocol spanning-tree mstp – enters MULTIPLE SPANNING TREE mode on the switch.

disable

Globally disable the multiple spanning tree protocol on the switch.

S5000

Syntax `disable`

To enable MSTP, enter the `no disable` command.

Defaults disabled.

Command Modes MULTIPLE SPANNING TREE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands [spanning-tree mstp](#) – enters MULTIPLE SPANNING TREE mode.

forward-delay

The amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.

S5000

Syntax `forward-delay seconds`

To return to the default setting, use the `no forward-delay` command.

Parameters

seconds	Enter the number of seconds the interface waits in the Blocking State and the Learning State before transiting to the Forwarding State. The range is 4 to 30. The default is **15 seconds**.

Defaults **15 seconds**

Command Modes MULTIPLE SPANNING TREE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

[max-age](#) – changes the wait time before MSTP refreshes protocol configuration information.

[hello-time](#) – changes the time interval between bridge protocol data units (BPDUs).

hello-time

Set the time interval between generation of MSTB bridge protocol data units (BPDUs).

S5000

Syntax `hello-time seconds`

To return to the default value, use the `no hello-time` command.

Parameters

seconds	Enter a number as the time interval between transmission of BPDUs. The range is 1 to 10. The default is **2 seconds**.

Defaults **2 seconds**

Command Modes MULTIPLE SPANNING TREE

Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	forward-delay – the amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State. max-age – changes the wait time before MSTP refreshes protocol configuration information.

max-age

Set the time interval for the MSTB to maintain configuration information before refreshing that information.

S5000

Syntax

```
max-age seconds
```

To return to the default values, use the `no max-age` command.

Parameters

max-age	Enter a number of seconds the FTOS waits before refreshing configuration information. The range is 6 to 40. The default is **20 seconds**.

Defaults	**20 seconds**
Command Modes	MULTIPLE SPANNING TREE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	forward-delay – the amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State. hello-time – changes the time interval between BPDUs.

max-hops

Configure the maximum hop count.

S5000

Syntax

```
max-hops number
```

To return to the default values, use the `no max-hops` command.

Parameters

range	Enter a number for the maximum hop count. The range is 1 to 40. The default is **20**.

Defaults	**20 hops**
Command Modes	MULTIPLE SPANNING TREE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	The `max-hops` command is a configuration command that applies to both the IST and all MST instances in the MSTP region. The BPDUs sent out by the root switch set the remaining-hops parameter to the configured value of max-hops. When a switch receives the BPDU, it decrements the received value of the remaining hops and uses the resulting value as remaining-hops in the BPDUs. If the remaining-hops reaches zero, the switch discards the BPDU and ages out any information that it holds for the port.

msti

Configure multiple spanning tree instance, bridge priority, and one or multiple VLANs mapped to the MST instance.

S5000

Syntax

`msti instance {vlan range | bridge-priority priority}`

To disable mapping or bridge priority, use the `no msti instance {vlan range | bridge-priority priority}` command.

Parameters

msti *instance*	Enter the MSTP instance. The range is zero (0) to 63.
vlan *range*	Enter the keyword `vlan` followed by the identifier range value. The range is 1 to 4094.
bridge-priority *priority*	Enter the keywords `bridge-priority` followed by a value in increments of 4096 as the bridge priority. The range is zero (0) to 61440. Valid priority values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

Defaults	default bridge-priority is **32768**.
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	By default, all VLANs are mapped to MST instance zero (0) unless you use the `vlan range` command to map it to a non-zero instance.

name

The name you assign to the multiple spanning tree region.

S5000

Syntax

`name region-name`

To remove the region name, use the `no name` command.

Parameters

region-name	Enter the MST region name. The range is 32 character limit.

Defaults

no default name.

Command Modes

MULTIPLE SPANNING TREE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

For two MSTP switches to be within the same MSTP region, the switches must share the same region name (including matching case).

Related Commands

msti – maps the VLAN(s) to an MST instance.

revision – assigns the revision number to the MST configuration.

protocol spanning-tree mstp

Enter MULTIPLE SPANNING TREE mode to enable and configure the multiple spanning tree group.

S5000

Syntax

`protocol spanning-tree mstp`

To disable the multiple spanning tree group, use the `no protocol spanning-tree mstp` command.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

MSTP is not enabled when you enter MULTIPLE SPANNING TREE mode. To enable MSTP globally on the switch, enter the `no disable` command while in MULTIPLE SPANNING TREE mode.

For more information about the multiple spanning tree protocol, refer to the *FTOS Configuration Guide*.

Example

```
FTOS(conf)#protocol spanning-tree mstp
FTOS(config-mstp)#no disable
```

Related Commands	disable – disables multiple spanning tree.

revision

The revision number for the multiple spanning tree configuration.

S5000

Syntax

`revision range`

To return to the default values, use the `no revision` command.

Parameters

range	Enter the revision number for the MST configuration. The range is 0 to 65535. The default is **0**.

Defaults	**0**
Command Modes	MULTIPLE SPANNING TREE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	For two MSTP switches to be within the same MST region, the switches must share the same revision number.
Related Commands	msti – maps the VLAN(s) to an MST instance. name – assigns the region name to the MST region.

show config

View the current configuration for the mode. Only non-default values are shown.

S5000

Syntax

`show config`

Command Modes	MULTIPLE SPANNING TREE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-mstp)#show config
!
protocol spanning-tree mstp
  no disable
  name CustomerSvc
  revision 2
  MSTI 10 VLAN 101-105
  max-hops 5
FTOS(conf-mstp)#
```

show spanning-tree mst configuration

View the multiple spanning tree configuration.

S5000

Syntax `show spanning-tree mst configuration`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information You must enable the multiple spanning tree protocol prior to using this command.

Example

```
FTOS#show spanning-tree mst configuration
MST region name: CustomerSvc
Revision: 2
MSTI VID
  10 101-105
FTOS#
```

show spanning-tree msti

View the multiple spanning tree instance.

S5000

Syntax `show spanning-tree msti [instance-number [brief]] [guard]`

Parameters

instance-number	(Optional) Enter the multiple spanning tree instance number. The range is 0 to 63.
brief	(Optional) Enter the keyword `brief` to view a synopsis of the MST instance.
guard	(Optional) Enter the keyword `guard` to display the type of guard enabled on an MSTP interface and the current port state.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must enable the multiple spanning tree protocol prior to using this command.

Example

```
FTOS#show spanning-tree msti 10
MSTI 10 VLANs mapped 101-105

Bridge Identifier has priority 32768, Address 0001.e802.3506
Configured hello time 2, max age 20, forward delay 15, max
hops 5
Current root has priority 16384, Address 0001.e800.0a5c
Number of topology changes 0, last change occurred 3058087

Port 82 (TenGigabitEthernet 2/0) is designated Forwarding
Port path cost 0, Port priority 128, Port Identifier 128.82
Designated root has priority 16384, address 0001.e800.0a:5c
Designated bridge has priority 32768, address 0001.e802.35:06
Designated port id is 128.82, designated path cost
Number of transitions to forwarding state 1
BPDU (Mrecords): sent 1109, received 0
The port is not in the portfast mode

Port 88 (TenGigabitEthernet 2/6) is root Forwarding
Port path cost 0, Port priority 128, Port Identifier 128.88
Designated root has priority 16384, address 0001.e800.0a:5c
Designated bridge has priority 16384, address 0001.e800.0a:5c
Designated port id is 128.88, designated path cost
Number of transitions to forwarding state 4
BPDU (Mrecords): sent 19, received 1103
The port is not in the portfast mode

Port 89 (TenGigabitEthernet 2/7) is alternate Discarding
Port path cost 0, Port priority 128, Port Identifier 128.89
Designated root has priority 16384, address 0001.e800.0a:5c
Designated bridge has priority 16384, address 0001.e800.0a:5c
Designated port id is 128.89, designated path cost
Number of transitions to forwarding state 3
BPDU (Mrecords): sent 7, received 1103
The port is not in the portfast mode
```

Example (EDS and LBK)

The bold line shows the loopback BPDU inconsistency (LBK_INC).

```
FTOS#show spanning-tree msti 0 brief
MSTI 0 VLANs mapped 1-4094

Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max
hops 20
Bridge ID Priority 32768, Address 0001.e801.6aa8
We are the root of MSTI 0 (CIST)
Configured hello time 2, max age 20, forward delay 15, max
hops 20
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0
```

```
Interface                            Designated
Name    PortID   Prio Cost Sts Cost Bridge ID      PortID
----------------------------------------------------------
Te 0/0  128.257  128  20000 EDS 0 32768 0001.e801.6aa8 128.257

Interface
Name  Role  PortID Prio Cost Sts Cost Link-type Edge Boundary
----------------------------------------------------------
Te 0/0 ErrDis 128.257  128 20000 EDS 0   P2P       No   No

FTOS#show spanning-tree msti 0
MSTI 0 VLANs mapped 1-4094

Root Identifier has priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max
hops 20
Bridge Identifier has priority 32768, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15, max
hops 20
We are the root of MSTI 0 (CIST)
Current root has priority 32768, Address 0001.e801.6aa8
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0
Number of topology changes 1, last change occured 00:00:15 ago
on Te 0/0
```

Port 257 (TenGigabitEthernet 0/0) is LBK_INC Discarding

```
Port path cost 20000, Port priority 128, Port Identifier
128.257
Designated root has priority 32768, address 0001.e801.6aa8
Designated bridge has priority 32768, address 0001.e801.6aa8
Designated port id is 128.257, designated path cost 0
Number of transitions to forwarding state 1
BPDU (MRecords): sent 21, received 9
The port is not in the Edge port mode
```

Usage Information

The following describes output for the `show spanning-tree msti 5 guard` command shown in the Example below.

Field	Description
Interface Name	MSTP interface.
Instance	MSTP instance.
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard).

Example (Guard)

```
FTOS#show spanning-tree msti 5 guard
Interface
Name    Instance  Sts Guard    type
-----------------------------------
Te 0/1  5         INCON(Root)  Rootguard
Te 0/2  5         FWD          Loopguard
Te 0/3  5         EDS(Shut)    Bpduguard
```

spanning-tree

Enable the multiple spanning tree protocol on the interface.

S5000

Syntax `spanning-tree`

To disable the multiple spanning tree protocol on the interface, use the `no spanning-tree` command.

Parameters

spanning-tree	Enter the keywords `spanning-tree` to enable the MSTP on the interface.

Defaults Enable.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

spanning-tree msti

Configure multiple spanning tree instance cost and priority for an interface.

S5000

Syntax `spanning-tree msti *instance* {cost *cost* | priority *priority*}`

Parameters

msti *instance*	Enter the keyword `msti` and the MST instance number. The range is zero (0) to 63.
cost *cost*	(OPTIONAL) Enter the keyword `cost` followed by the port cost value. The range is 1 to 200000. The defaults are: • 1-Gigabit Ethernet interface = **20000** • 10-Gigabit Ethernet interface = **2000** • 40-Gigabit Ethernet interface = **2000** • Port Channel interface with one 1-Gigabit Ethernet interface = **20000** • Port Channel interface with one 10-Gigabit Ethernet = **2000** • Port Channel interface with one 40-Gigabit Ethernet = **2000** • Port Channel interface with two 1-Gigabit Ethernet = **18000** • Port Channel with two 10-Gigabit Ethernet = **1800** • Port Channel with two 40-Gigabit Ethernet = **1800**
priority *priority*	Enter keyword `priority` followed by a value in increments of 16 as the priority. The range is 0 to 240. The default is **128**.

Defaults

- cost = depends on the interface type
- priority = **128**

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

spanning-tree mstp

Configures a Layer 2 MSTP interface as an edge port with (optionally) a bridge protocol data unit (BPDU) guard, or enables the root guard or loop guard feature on the interface.

S5000

Syntax

```
spanning-tree mstp {edge-port [bpduguard [shutdown-on-
violation]] | loopguard | rootguard}
```

Parameters

edge-port	Enter the keywords `edge-port` to configure the interface as a multiple spanning tree edge port.
bpduguard	(OPTIONAL) Enter the keyword `portfast` to enable Portfast to move the interface into forwarding mode immediately after the root fails. Enter the keyword `bpduguard` to disable the port when it receives a BPDU.
shutdown-on-violation	(OPTIONAL) Enter the keywords `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.
loopguard	Enter the keyword `loopguard` to enable STP loop guard on an MSTP port or port-channel interface.
rootguard	Enter the keyword `rootguard` to enable root guard on an MSTP port or port-channel interface.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

On an MSTP switch, a port configured as an edge port immediately transitions to the forwarding state. Only ports connected to end-hosts should be configured as an edge port. Consider an edge port similar to a port with `spanning-tree portfast` enabled.

If you do not enable `shutdown-on-violation`, BPDUs are still sent to the stack-unit CPU.

Root guard and loop guard cannot be enabled at the same time on a port. For example, if you configure loop guard on a port on which root guard is already configured, the following error message is displayed: `% Error: RootGuard is configured. Cannot configure LoopGuard`.

When used in an MSTP network, if root guard blocks a boundary port in the CIST, the port is also blocked in all other MST instances.

Enabling Portfast BPDU guard and loop guard at the same time on a port results in a port that remains in a blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an err-disabled blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a loop-inconsistent blocking state and no traffic is forwarded on the port.

tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

S5000

Syntax

`tc-flush-standard`

To disable, use the `no tc-flush-standard` command.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

By default, FTOS implements an optimized flush mechanism for MSTP. This helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, this `knob` command can be turned on to enable flushing MAC addresses after receiving every topology change notification.

34

Multicast

FTOS supports multicast commands on the S5000 switch.

This chapter contains the following sections:

- IPv4 Multicast Commands
- IPv6 Multicast Commands

IPv4 Multicast Commands

The following section contains the IPv4 multicast commands.

clear ip mroute

Clear learned multicast routes on the multicast forwarding table. To clear the protocol-independent multicast (PIM) tree information base, use the `clear ip pim tib` command.

S5000

Syntax `clear ip mroute {group-address [source-address] | *}`

Parameters

***group-address* [*source-address*]**	Enter the multicast group address and source address (if desired), in dotted decimal format, to clear information on a specific group.
*****	Enter * to clear all multicast routes.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands show ip pim tib – shows the PIM tree information base.

ip mroute

Assign a static mroute.

S5000

Syntax

`ip mroute destination mask {ip-address | null 0| {{bgp| ospf} process-id | isis | rip | static} {ip-address | tag | null 0}} [distance]`

To delete a specific static mroute, use the `ip mroute destination mask {ip-address | null 0| {{bgp| ospf} process-id | isis | rip | static} {ip-address | tag | null 0}} [distance]` command.

To delete all mroutes matching a certain mroute, use the `no ip mroute destination mask` command.

Parameters

destination	Enter the IP address in dotted decimal format of the destination device.
mask	Enter the mask in slash prefix formation (/x) or in dotted decimal format.
null 0	(OPTIONAL) Enter the keyword `null` followed by zero (0).
[*protocol* [*process-id* | *tag*] *ip-address*]	(OPTIONAL) Enter one of the routing protocols: • Enter the BGP as-number followed by the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor. The range is 1 to 65535. • Enter the OSPF process identification number followed by the IP address in dotted decimal format of the RPF neighbor. the range is 1 to 65535. • Enter the IS-IS alphanumeric tag string followed by the IP address in dotted decimal format of the RPF neighbor. • Enter the RIP IP address in dotted decimal format of the RPF neighbor.
static *ip-address*	(OPTIONAL) Enter the Static IP address in dotted decimal format of the RPF neighbor.
ip-address	(OPTIONAL) Enter the IP address in dotted decimal format of the RPF neighbor.
distance	(OPTIONAL) Enter a number as the distance metric assigned to the mroute. The range is 0 to 255.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip multicast-limit

Use this feature to limit the number of multicast entries on the system.

S5000

Syntax

```
ip multicast-limit limit
```

Parameters

limit	Enter the desired maximum number of multicast entries on the system. The range is 1 to 2000.

Defaults 400

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This features allows you to limit the number of multicast entries on the system. This number is the sum total of all the multicast entries on all stack-units in the system. For each stack-unit, the multicast module only installs the maximum possible number of entries, depending on the configured CAM profile.

Use the IN-L3-McastFib CAM partition to store multicast routes. It is a separate hardware limit that exists per port-pipe. Any software-configured limit might be superseded by this hardware space limitation. The opposite is also true, the CAM partition might not be exhausted at the time the system-wide route limit set by the `ip multicast-limit` command is reached.

Related Commands

show ip igmp groups – shows the IGMP groups.

ip multicast-routing

Enable IP multicast forwarding.

S5000

Syntax

```
ip multicast-routing
```

To disable multicast forwarding, use the `no ip multicast-routing` command.

Defaults Disabled.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

After you enable multicast, you can enable IGMP and PIM on an interface. In INTERFACE mode, enter the `ip pim sparse-mode` command to enable IGMP and PIM on the interface.

Related Commands

[ip pim sparse-mode](#) – enables IGMP and PIM on an interface.

show ip mroute

View the multicast routing table.

S5000

Syntax

```
show ip mroute [static | group-address [source-address] |
active [rate] | summary]
```

Parameters

static	(OPTIONAL) Enter the keyword `static` to view static multicast routes.
***group-address* [*source-address*]**	(OPTIONAL) Enter the multicast group-address to view only routes associated with that group. Enter the source-address to view routes with that group-address and source-address.
active [*rate*]	(OPTIONAL) Enter the keyword `active` to view only active multicast routes. Enter a rate to view active routes over the specified rate. The range is 0 to 10000000.
summary	(OPTIONAL) Enter the keyword `summary` to view routes in a tabular format.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (Static)

```
FTOS#show ip mroute static

Mroute: 23.23.23.0/24, interface: Lo 2
Protocol: static, distance: 0, route-map: none, last change:
00:00:23
```

Example (Snooping)

```
FTOS#show ip mroute snooping

IPv4 Multicast Snooping Table

(*, 224.0.0.0), uptime 17:46:23
  Incoming vlan: Vlan 2
  Outgoing interface list:
    TenGigabitEthernet 4/13

(*, 225.1.2.1), uptime 00:04:16
  Incoming vlan: Vlan 2
  Outgoing interface list:
    TenGigabitEthernet 4/11
    TenGigabitEthernet 4/13

(165.87.1.7, 225.1.2.1), uptime 00:03:17
  Incoming vlan: Vlan 2
  Outgoing interface list:
    TenGigabitEthernet 4/11
    TenGigabitEthernet 4/13
    TenGigabitEthernet 4/20
```

Usage Information

The following describes output for the `show ip mroute` command shown in the Example below.

Field	Description
(S, G)	Displays the forwarding entry in the multicast route table.
uptime	Displays the amount of time the entry has been in the multicast forwarding table.
Incoming interface	Displays the reverse path forwarding (RPF) information towards the source for (S,G) entries and the RP for (*,G) entries.
Outgoing interface list:	Lists the interfaces that meet one of the following: • a directly connected member of the Group • statically configured member of the Group • received a (*,G) or (S,G) Join message

Example

```
FTOS#show ip mroute

IP Multicast Routing Table

(*, 224.10.10.1), uptime 00:05:12
  Incoming interface: TenGigabitEthernet 3/12
  Outgoing interface list:
    TenGigabitEthernet 3/13

(1.13.1.100, 224.10.10.1), uptime 00:04:03
  Incoming interface: TenGigabitEthernet 3/4
  Outgoing interface list:
    TenGigabitEthernet 3/12
    TenGigabitEthernet 3/13

(*, 224.20.20.1), uptime 00:05:12
  Incoming interface: TenGigabitEthernet 3/12
  Outgoing interface list:
    TenGigabitEthernet 3/4
```

show ip rpf

View reverse path forwarding.

S5000

Syntax `show ip rpf`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Static mroutes are used by network administrators to control the reach-ability of the multicast sources. If a PIM-registered multicast source is reachable using static mroute as well as unicast route, the distance of each route is examined and the route with shorter distance is the one the PIM selects for reach-ability.

NOTE: The default distance of mroutes is zero (0) and is CLI configurable on a per route basis.

Example

```
FTOS#show ip rpf
RPF information for 10.10.10.9
  RPF interface: Te 3/4
  RPF neighbor: 165.87.31.4
  RPF route/mask: 10.10.10.9/255.255.255.255
  RPF type: unicast
```

IPv6 Multicast Commands

The following section contains the IPv6 multicast commands.

ip multicast-limit

Use this feature to limit the number of multicast entries on the system.

S5000

Syntax `ip multicast-limit` *`limit`*

Parameters

limit	Enter the desired maximum number of multicast entries on the system. The range is 1 to 2000.

Defaults	**400**
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	This features allows you to limit the number of multicast entries on the system. This number is the sum total of all the multicast entries on all stack-units in the system. For each stack-unit, the multicast module only installs the maximum possible number of entries, depending on the configured CAM profile. Use the IN-L3-McastFib CAM partition to store multicast routes. It is a separate hardware limit that exists per port-pipe. Any software-configured limit might be superseded by this hardware space limitation. The opposite is also true, the CAM partition might not be exhausted at the time the system-wide route limit set by the `ip multicast-limit` command is reached.
Related Commands	show ip igmp groups – shows the IGMP groups.

35

Neighbor Discovery Protocol (NDP)

FTOS supports Neighbor Discovery Protocol for IPv6 on the S5000 switch.

NDP for IPv6 is defined in RFC 2461 as part of the Stateless Address Autoconfiguration protocol. It replaces the Address Resolution Protocol used with IPv4. NDP defines mechanisms for solving the following problems:

- Router discovery: Hosts can locate routers residing on a link
- Prefix discovery: Hosts can discover address prefixes for the link
- Parameter discovery
- Address autoconfiguration — configuration of addresses for an interface
- Address resolution — mapping from IP address to link-layer address
- Next-hop determination
- Neighbor unreachability detection (NUD): Determine that a neighbor is no longer reachable on the link.
- Duplicate address detection (DAD): Allow a node to check whether a proposed address is already in use.
- Redirect: The router can inform a node about a better first-hop.

NDP makes use of the following five ICMPv6 packet types in its implementation:

- Router Solicitation
- Router Advertisement
- Neighbor Solicitation
- Neighbor Advertisement
- Redirect

clear ipv6 neighbors

Delete all entries in the IPv6 neighbor discovery cache or neighbors of a specific interface. Static entries are not removed using this command.

S5000

Syntax `clear ipv6 neighbors [ipv6-address] [type slot/port]`

Parameters

ipv6-address	Enter the IPv6 address of the neighbor in the x:x:x:x::x format to remove a specific IPv6 neighbor. **NOTE:** The :: notation specifies successive hexadecimal fields of zero. Only one occurrence of this notation is permitted in an IPv6 address.

interface *type slot/port*	To remove all neighbor entries learned on a specific interface, enter the keyword `interface` followed by the interface type and slot/ port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

ipv6 nd mtu

Configure an IPv6 neighbor discovery.

S5000

Syntax `ipv6 nd mtu` *`number`*

Parameters

mtu *number*	Set the MTU advertisement value in Routing Prefix Advertisement packets. The range is 1280 to 9234.

Defaults none

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `ip nd mtu` command sets the value advertised to routers. It does not set the actual MTU rate. For example, if `ip nd mtu` is set to 1280, the interface still passes 1500-byte packets.

The `mtu` command sets the actual frame size passed and can be larger than the advertised MTU. If the mtu setting is larger than the `ip nd mtu` command, an error message is sent, but the configuration is accepted. The error message is: `% Error: nd ra mtu is greater than link mtu, link mtu will be used.`

Related Commands mtu – sets the maximum link MTU (frame size) for an Ethernet interface.

ipv6 neighbor

Configure a static entry in the IPv6 neighbor discovery.

S5000

Syntax

`ipv6 neighbor {`*`ipv6-address`*`} {`*`interface-type slot/port`*`} {`*`hardware_address`*`}`

To remove a static IPv6 entry from the IPv6 neighbor discovery, use the `no ipv6 neighbor {`*`ipv6-address`*`} {`*`interface-type slot/port`*`}` command.

Parameters

ipv6-address	Enter the IPv6 address of the neighbor in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zero.
interface-type slot/port	Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
hardware_address	Enter a 48-bit hardware MAC address in nn:nn:nn:nn:nn:nn format.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ipv6 neighbors

Display IPv6 discovery information. Entering the command without options shows all IPv6 neighbor addresses stored on the control processor (CP).

S5000

Syntax

`show ipv6 neighbors [`*`ipv6-address`*`] [interface `*`type slot/port`*`]`

Parameters

ipv6-address	Enter the IPv6 address of the neighbor in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zero.
interface *type slot/port*	Enter the keyword `interface` followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers. The port is 0. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ipv6 neighbors

IPv6 Address Expires(min) HardwareAddress State Interface/VLAN/
CPU
---------------------------------------------------------
fe80::201:e8ff:fe17:5bc6
             1439    00:01:e8:17:5b:c6 STALE  Te 1/9    -   CP
fe80::201:eff:fe17:5bc7
             1439    00:01:e8:17:5b:c7 STALE  Te 1/10   -   CP
fe80::201:e8ff:fe17:5bc8
             1439    00:01:e8:17:5b:c8 STALE  Te 1/11   -   CP
fe80::201:e8ff:fe17:5caf
             0.3     00:01:e8:17:5c:af REACH  Po 1      -   CP
```

```
fe80::201:e8ff:fe17:5cb0
             1439    00:01:e8:17:5c:b0 STALE  Po 32     -   CP
fe80::201:e8ff:fe17:5cb1
             1439    00:01:e8:17:5c:b1 STALE  Po 255    -   CP
fe80::201:e8ff:fe17:5cae
             1439    00:01:e8:17:5c:ae STALE  Te 1/3 Vl 100 CP
fe80::201:e8ff:fe17:5cae
             1439    00:01:e8:17:5c:ae STALE  Te 1/5 Vl 1000 CP
fe80::201:e8ff:fe17:5cae
             1439    00:01:e8:17:5c:ae STALE Te 1/7  Vl 2000 CP

FTOS#
```

36

NPIV Proxy Gateway

The N-port identifier virtualization (NPIV) Proxy Gateway (NPG) feature provides FCoE-FC bridging capability on the S5000 switch, allowing server CNAs to communicate with SAN fabrics over the S5000.

To configure the S5000 to operate as an NPIV proxy gateway, use the following commands:

dcb-map

Create a DCB map to configure priority flow control (PFC) and enhanced transmission selection (ETS) on Ethernet ports that support converged Ethernet traffic. Apply the DCB map to an Ethernet interface.

S5000

Syntax `dcb-map map-name`

Parameters

map-name	Enter a DCB map name. The maximum number of alphanumeric characters is 32.

Defaults None. There are no pre-configured PFC and ETS settings on S5000 Ethernet interfaces.

Command Modes CONFIGURATION

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

A DCB map is a template used to configure DCB parameters and apply them on converged Ethernet interfaces. DCB parameters include priority-based flow control (PFC) and enhanced traffic selection (ETS).

To display the PFC and ETS settings in DCB maps, enter the `show qos dcb-map` command.

Use the `dcb-map` command to create a DCB map to specify PFC and ETS settings and apply it on Ethernet ports. After you apply a DCB map to an interface, the PFC and ETS settings in the map are applied when the Ethernet port is enabled. DCBx is enabled on Ethernet ports by default.

The `dcb-map` command is supported only on physical Ethernet interfaces.

To remove a DCB map from an interface, enter the `no dcb-map map-name` command in Interface configuration mode.

Related Commands

show qos dcb-map– displays the dcb-map profiles configured on the system.

dcb-map stack-unit all stack-ports all– applies a DCB map on all ports of a switch stack.

description

In an FCoE map, add a text description of the FCoE and FC parameters used to transmit storage traffic over an S5000 NPIV proxy gateway in a converged fabric.

S5000

Syntax `description text`

Parameters

text	Enter a maximum of 32 characters.

Defaults None

Command Modes FCOE MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The text description is displayed in `show fcoe-map` command output.

Related Commands

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

fabric

Apply an FCoE map on a fabric-facing Fibre Channel (FC) port.

S5000

Syntax `fabric map-name`

Parameters

map-name	Maximum: 32 alphanumeric characters.

Defaults None

Command Modes INTERFACE FIBRE_CHANNEL

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information An FCoE map is a template used to map FCoE and FC parameters in a converged fabric. An FCoE map is used to virtualize upstream FC ports on an S5000 NPIV proxy gateway so that they appear to downstream server CNA ports as FCoE forwarder (FCF) ports on an FCoE network. When applied to FC and Ethernet ports on an NPIV proxy gateway, an FCoE map allows the switch to operate as an FCoE-FC bridge between an FC SAN and an FCoE network by providing

FCoE-enabled servers and switches with the necessary parameters to log in to a SAN fabric. Use the `fcoe-map` command to create an FCoE map.

On an S5000 NPIV proxy gateway, an FCoE map is applied on fabric-facing FC ports and server-facing Ethernet ports. Use the `fabric` command to apply an FCoE map on an FC port. Use the `fcoe-map` command to apply an FCoE map on an Ethernet port.

After you apply an FCoE map on an FC interface, when the port is enabled (`no shutdown`), the NPIV proxy gateway starts sending FIP multicast advertisements on behalf of the FC port to downstream servers in order to advertise the availability of a new FCF port on the FCoE VLAN.

To remove an FCoE map from an FC interface, enter the `no fabric` *`map-name`* command in Interface configuration mode.

Related Commands

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

interface fibrechannel — configures a Fibre Channel interface on the switch. .

show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

fabric-id vlan

In an FCoE map, configure the association between the dedicated VLAN used to carry FCoE traffic between servers and a SAN, and the fabric where the desired storage arrays are installed.

S5000

Syntax

`fabric-id` *`fabric-num`* `vlan` *`vlan-id`*

Parameters

fabric-id *fabric-num*	Enter a fabric ID number that is the same as the ID number of the dedicated VLAN used to carry FCoE storage traffic to the fabric specified in the FCoE map.
vlan*vlan-id*	Enter the ID number of the dedicated VLAN used to carry FCoE storage traffic between servers and a SAN fabric and specified with the `vlan` command in the FCoE map.

Defaults

None

Command Modes

FCOE MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

In the `fabric-id vlan` command, the fabric and VLAN ID numbers must be the same.

In each FCoE map, the fabric ID, FC-MAP value, and FCoE VLAN parameters must be unique.

To remove a fabric-VLAN association from an FCoE map, enter the `no fabric-id vlan` command.

Related Commands

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

fc-map

In an FCoE map, configure the FCoE mapped address prefix (FC-MAP) value which is used to identify FCoE traffic transmitted on the FCoE VLAN for the specified fabric.

S5000

Syntax

`fc—map fc-map-value`

Parameters

fc-map-value	Enter the unique MAC address prefix used by a SAN fabric. The range of FC-MAP values is from 0EFC00 to 0ECFF.

Defaults

None

Command Modes

FCOE MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The FC-MAP value you enter must match the FC-MAP value used by an FC switch or FCoE forwarder (FCF) in the fabric. An FC switch accepts only FCoE traffic that uses the correct FC-MAP value.

The FC-MAP value is used to generate the fabric-provided MAC address (FP-MAC). The FPMA is used by servers to transmit FCoE traffic to the fabric. An FC-MAP can be associated with only one FCoE VLAN and vice versa.

In an FCoE map, the FC-MAP value, fabric ID, and FCoE VLAN parameters must be unique.

To remove a configured FC-MAP value from an FCoE map, enter the `no fc-map` command.

Related Commands

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

fcf-priority

In an FCoE map, configure the priority used by a server CNA to select an upstream FCoE forwarder (FCF).

S5000

Syntax `fcf—priority priority`

Parameters

priority	Enter the priority assigned to the S5000 NPIV proxy gateway, which appears to a downstream server CNA as an FCF. The range of FCF priority values is from 1 to 255.

Defaults 128

Command Modes FCOE MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The FCF priority you assign to an S5000 is used by server CNAs to select an upstream FCF to use for a fabric login (FLOGI).

To remove a configured FCF priority from an FCoE map, enter the `no fcf-priority` command.

Related Commands

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

fcoe-map

Create an FCoE map which contains the parameters used to configure the links between server CNAs and a SAN fabric. Apply the FCoE map on a server-facing Ethernet port.

S5000

Syntax `fcoe-map map-name`

Parameters

map-name	Maximum: 32 alphanumeric characters.

Defaults None

Command Modes

CONFIGURATION

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

An FCoE map is a template used to map FCoE and FC parameters in a converged fabric. An FCoE map is used to virtualize upstream FC ports on an S5000 NPIV proxy gateway so that they appear to downstream server CNA ports as FCoE forwarder (FCF) ports on an FCoE network. When applied to FC and Ethernet ports on an NPIV proxy gateway, an FCoE map allows the switch to operate as an FCoE-FC bridge between an FC SAN and an FCoE network by providing FCoE-enabled servers and switches with the necessary parameters to log in to a SAN fabric.

On an S5000 NPIV proxy gateway, an FCoE map is applied on fabric-facing FC ports and server-facing Ethernet ports. Use the `fcoe-map` command to apply an FCoE map on an Ethernet port. Use the `fabric` command to apply an FCoE map on an FC port.

An FCoE map consists of the following parameters: the dedicated FCoE VLAN used for storage traffic, the destination SAN fabric (FC-MAP value), FCF priority used by a server, and the FIP keepalive (FKA) advertisement timeout.

In each FCoE map, the fabric ID, FC-MAP value, and FCoE VLAN parameters must be unique. Use one FCoE map to access one SAN fabric. You cannot use the same FCoE map to access different fabrics.

To remove an FCoE map from an Ethernet interface, enter the `no fcoe-map` *`map-name`* command in Interface configuration mode.

Related Commands

interface fibrechannel — configures a Fibre Channel interface on the switch.

show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

feature fc

Enable Fibre Channel capability on the S5000.

S5000

Syntax

```
feature fc
```

Defaults

The S5000 is not enabled to operate in Fibre Channel mode.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use this command to configure the S5000 to interoperate with Fibre Channel devices in SAN fabrics.

Enter the `no feature fc` command to disable the Fibre Channel command-line interface and free memory resources allocated to Fibre Channel operation.

Example

```
FTOS(conf)#feature fc
```

Related Commands

show interfaces fibrechannel — displays the configuration of a Fibre Channel interface.

fka-adv-period

In an FCoE map, configure the time interval used to transmit FIP keepalive (FKA) advertisements.

S5000

Syntax `fka-adv-period seconds`

Parameters

seconds	Enter the time period (in seconds) used to send FIP keepalive messages to peer devices. The range is from 8 to 90 seconds.

Defaults 8 seconds

Command Modes FCOE MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information To delete the FIP keepalive time period from an FCoE map, enter the `no fka-adv-erpiod` command.

Related Commands

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

interface vlan (NPIV proxy gateway)

Create a dedicated VLAN to be used to send and receive Fibre Channel traffic over FCoE links between servers and a fabric over an S5000 NPIV proxy gateway.

S5000

Syntax `interface vlan vlan-id`

Parameters

vlan-id	Enter a number as the VLAN Identifier. The range is 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000 configured as an NPIV proxy gateway.

Usage Information FCoE storage traffic received from servers on an S5000 NPIV proxy gateway is de-capsulated into Fibre Channel packets and forwarded over FC links to SAN switches in a specified fabric. You must configure a separate FCoE VLAN for each fabric to which FCoE traffic is forwarded. Any non-FCoE traffic sent on a dedicated FCoE VLAN will be dropped.

You configure the association between a dedicated VLAN, which carries FCoE traffic from server CNAs over the NPIV proxy gateway to a SAN fabric in which destination storage arrays are installed, in an FCoE map by using the `fabric id vlan` command.

When you apply an FCoE map to a server-facing Ethernet port, the port is automatically configured as a tagged member of the FCoE VLAN.

For more information about VLANs and the commands to configure them, refer to the Virtual LAN (VLAN) Commands section of the Layer 2 chapter.

Example (Single Range)

```
FTOS(conf)#interface vlan 10
FTOS(conf-if-vl-3)#
```

Related Commands

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

keepalive

In an FCoE map, enable the monitoring of FIP keepalive messages (if it is disabled).

S5000

Syntax `keepalive`

Parameters None

Defaults FIP keepalive monitoring is enabled on Ethernet and Fibre Channel interfaces.

Command Modes FCOE MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

FIP keepalive (FKA) messaging is used to detect if other FCoE devices are reachable.

To remove FIP keepalive monitoring from an FCoE map, enter the `no keepalive` command.

Related Commands

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

show fcoe-map— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

priority-pgid

Assign 802.1p priority traffic to a priority group in a DCB map.

S5000

Syntax	`priority-pgid` *`dot1p0_group-num dot1p1_group-num dot1p2_group-num dot1p3_group-num dot1p4_group-num dot1p5_group-num dot1p6_group-num dot1p7_group-num`*

Parameters

dot1p0_group-num	Enter the priority group number for each 802.1p class of traffic in a DCB map.
dot1p1_group-num	
dot1p2_group-num	
dot1p3_group-num	
dot1p4_group-num	
dot1p5_group-num	
dot1p6_group-num	
dot1p7_group-num	

Defaults	None
Command Modes	DCB MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

PFC and ETS settings are not pre-configured on Ethernet ports. You must use the `dcb-map` command to configure different groups of 802.1p priorities with PFC and ETS settings.

Using the `priority-pgid` command, you assign each 802.1p priority to one priority group. A priority group consists of 802.1p priority values that are grouped together for similar bandwidth allocation and scheduling, and that share latency and loss requirements. All 802.1p priorities mapped to the same queue must be in the same priority group. For example, the `priority-pgid 0 0 0 1 2 4 4 4` command creates the following groups of 802.1p priority traffic:

- Priority group 0 contains traffic with dot1p priorities 0, 1, and 2.
- Priority group 1 contains traffic with dot1p priority 3.
- Priority group 2 contains traffic with dot1p priority 4.

- Priority group 4 contains traffic with dot1p priority 5, 6, and 7.

To remove a priority-pgid configuration from a DCB map, enter the `no priority-pgid` command.

Related Commands	dcb-map — creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports. priority-group bandwidth pfc— configures the ETS bandwidth allocation and the PFC setting used to manage the port traffic in an 802.1p priority group.

priority-group bandwidth pfc

Configure the ETS bandwidth allocation and PFC mode used to manage port traffic in an 802.1p priority group.

S5000

Syntax

```
priority-group group-num {bandwidth percentage| strict-
priority} pfc {on | off}
```

Parameters

priority-group *group-num*	Enter the keyword `priority-group` followed by the number of an 802.1p priority group. Use the `priority-pgid` command to create the priority groups in a DCB map.
bandwidth *percentage*	Enter the keyword `bandwidth` followed by a bandwidth percentage allocated to the priority group. The range of valid values is 1 to 100. The sum of all allocated bandwidth percentages in priority groups in a DCB map must be 100%.
strict-priority	Configure the priority-group traffic to be handled with strict priority scheduling. Strict-priority traffic is serviced first, before bandwidth allocated to other priority groups is made available.
pfc {on | off}	Configure whether priority-based flow control is enabled (on) or disabled (off) for port traffic in the priority group.

Defaults None

Command Modes DCB MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `dcb-map` command to configure priority groups with PFC and/or ETS settings and apply them to Ethernet interfaces.

Use the `priority-pgid` command to map 802.1p priorities to a priority group. You can assign each 802.1p priority to only one priority group. A priority group consists of 802.1p priority values that are grouped together for similar bandwidth allocation and scheduling, and that share latency and loss requirements. All 802.1p priorities mapped to the same queue must be in the same priority group.

Repeat the `priority-group bandwidth pfc` command to configure PFC and ETS traffic handling for each priority group in a DCB map.

You can enable PFC on a maximum of two priority queues.

If you configure more than one priority group as strict priority, the higher numbered priority queue is given preference when scheduling data traffic.

If a priority group does not use its allocated bandwidth, the unused bandwidth is made available to other priority groups.

To remove a priority-group configuration in a DCB map, enter the `no priority-group bandwidth pfc` command.

By default, equal bandwidth is assigned to each dot1p priority in a priority group. Use the `bandwidth` parameter to configure the bandwidth percentage assigned to a priority group. The sum of the bandwidth allocated to all priority groups in a DCB map must be 100% of the bandwidth on the link. You must allocate at least 1% of the total port bandwidth to each priority group.

Related Commands

dcb-map – creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports.

priority-pgid – configures the 802.1p priority traffic in a priority group for a DCB map.

show fcoe-map

Display the Fibre Channel and FCoE configuration parameters in FCoE maps.

S5000

Syntax

`show fcoe-map [brief | map-name]`

Parameters

brief	Displays an overview of currently configured FCoE maps.
map-name	Displays the FC and FCoE configuration parameters in a specified FCoE map. The FCoE map is applied on Ethernet (FCoE) and FC ports to transmit FC storage traffic to a specified fabric.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `show fcoe-map` command to display the FC and FCoE parameters used to configure server-facing Ethernet (FCoE) and fabric-facing FC ports in all FCoE maps on an S5000 NPIV proxy gateway.

In each FCoE map, the values for the fabric ID and FC-MAP that identify the SAN fabric to which FC storage traffic is sent, and the FCoE VLAN to be used must be unique.

An FCoE map is used to identify the SAN fabric to which FCoE storage traffic is sent and to virtualize S5000 FC ports so that they appear to downstream server CNA ports as FCoE Forwarder (FCF) ports on an FCoE network.

The following table describes the `show fcoe-map brief` and `show fcoe-map` *`map-name`* output shown in the examples below.

Field	**Description**
Fabric-Name	Name of a SAN fabric.
Fabric ID	The ID number of the SAN fabric to which FC traffic is forwarded.
VLAN ID	The dedicated FCoE VLAN used to transport FCoE storage traffic between servers and a fabric over the NPIV proxy gateway. The configured VLAN ID must be the same as the fabric ID.
VLAN priority	FCoE traffic uses VLAN priority 3. (This setting is not user-configurable.)
FC-MAP	FCoE MAC address-prefix value - The unique 24-bit MAC address prefix that identifies a fabric.
FKA-ADV-period	Time interval (in seconds) used to transmit FIP keepalive advertisements.
FCF Priority	The priority used by a server to select an upstream FCoE forwarder.
Config-State	Indicates whether the configured FCoE and FC parameters in the FCoE map are valid: Active (all mandatory FCoE and FC parameters are correctly configured) or Incomplete (either the FC-MAP value, fabric ID, or VLAN ID are not correctly configured).
Oper-State	Operational status of link to the fabric: Up (link is up and transmitting FC traffic), Down (link is down and not transmitting FC traffic), Link-wait (link is up and waiting for FLOGI to complete on peer FC port), or Removed (port has been shut down).
Members	S5000 Ethernet and FC ports that are members of the dedicated FCoE VLAN that carries storage traffic to the specified fabric.

Example

```
FTOS# show fcoe-map brief
Fabric Fabric Vlan FC-MAP    FCF      Active State
Name    ID     ID           Priority
Fabric1  1    1002 0x0EFC00  128      Y      Up (at least 1 FC
port is up)
Fabric2  2    1003 0x0EFC01  128      Y      Down
Fabric3  2    1004 0x0EFC02  128      N      Down

FTOS# show fcoe-map fabric1
Fabric Name      FABRIC_NAME_1
Fabric id        1002
Vlan id          1002
Vlan priority    3
FC-MAP           0x0EFC00
FKA-ADV-period   8000ms
Operational-Mode Up
Members
TE0/1 TE0/2 FC0/1 FC0/2 FC0/3 FC0/4
```

Related Commands	fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

show npiv devices

Display the FCoE and FC devices currently logged in to an S5000 NPIV proxy gateway.

S5000

Syntax `show npiv devices [brief]`

Parameters

brief	Displays an overview of current server CNA-fabric connections over an S5000 NPIV proxy gateway.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `show npiv devices` command to display information on the server CNA, server-facing Ethernet and fabric-facing FC ports, and the SAN fabric in each server-fabric connection over an S5000 NPIV proxy gateway.

The following table describes the `show npiv devices brief` output shown in the example below.

Field	**Description**
ENode-Intf	S5000 Ethernet interface (*slot/port*) to which a server CNA is connected.
ENode-WWPN	Worldwide port name (WWPN) of a server CNA port.
FCoE-Vlan	VLAN ID of the dedicated VLAN used to transmit FCoE traffic to and from the fabric.
Fabric-Intf	Fabric-facing Fibre Channel port (*slot/port*) on which FC traffic is transmitted to the specified fabric.
Fabric-Map	Name of the FCoE map containing the FCoE/FC configuration parameters for the server CNA-fabric connection.
LoginMethod	Method used by the server CNA to log in to the fabric; for example: FLOGI - ENode logged in using a fabric login (FLOGI). FDISC - ENode logged in using a fabric discovery (FDISC).

Field	Description
Status	Operational status of the link between a server CNA port and a SAN fabric: Logged In - Server has logged in to the fabric and is able to transmit FCoE traffic.

Example

```
FTOS# show npiv devices brief

Total NPIV Devices = 2
---------------------------------------------------------------
----------------------------

ENode-Intf  ENode-WWPN           FCoE-Vlan  Fabric-Intf
Fabric-Map   LoginMethod  Status
---------------------------------------------------------------
---------------------------

Te 0/12     20:01:00:10:18:f1:94:20   1003      Fc 0/5
fid_1003     FLOGI       LOGGED_IN
Te 0/13     10:00:00:00:c9:d9:9c:cb   1003      Fc 0/0
fid_1003     FDISC       LOGGED_IN
```

Usage Information

The following table describes the `show npiv devices` output shown in the example below.

Field	Description
ENode [*number*]	A server CNA that has successfully logged in to a fabric over an S5000 Ethernet port in ENode mode.
Enode MAC	MAC address of a server CNA port.
Enode Intf	Port number of a server-facing Ethernet port operating in ENode mode.
FCF MAC	Fibre Channel forwarder MAC: MAC address of S5000 FCF interface.
Fabric Intf	Fabric-facing Fibre Channel port (*slot/port*) on which FCoE traffic is transmitted to the specified fabric.
FCoE VLAN	ID of the dedicated VLAN used to transmit FCoE traffic from a server CNA to a fabric and configured on both the server-facing S5000 port and server CNA port.
Fabric Map	Name of the FCoE map containing the FCoE/FC configuration parameters for the server CNA-fabric connection.
Enode WWPN	Worldwide port name of the server CNA port.
Enode WWNN	Worldwide node name of the server CNA.
FCoE MAC	Fabric-provided MAC address (FPMA). The FPMA consists of the FC-MAP value in the FCoE map and the FC-ID provided by the fabric after a successful FLOGI. In the FPMA, the most significant bytes are the FC-MAP; the least significant bytes are the FC-ID.
FC-ID	FC port ID provided by the fabric.

Field	Description
LoginMethod	Method used by the server CNA to log in to the fabric; for example, FLOGI or FDISC.
Secs	Number of seconds that the fabric connection is up.
State	Status of the fabric connection: logged in.

Example

```
ENode[0]:
ENode MAC     :     00:10:18:f1:94:21
ENode Intf    :     Te 0/12
FCF MAC       :     5c:f9:dd:ef:10:c8
Fabric Intf   :     Fc 0/5
FCoE Vlan     :     1003
Fabric Map    :     fid_1003
ENode WWPN    :     20:01:00:10:18:f1:94:20
ENode WWNN    :     20:00:00:10:18:f1:94:21
FCoE MAC      :     0e:fc:03:01:02:01
FC-ID         :     01:02:01
LoginMethod   :     FLOGI
Secs          :     5593
Status        :     LOGGED_IN

ENode[1]:
ENode MAC     :     00:10:18:f1:94:22
ENode Intf    :     Te 0/13
FCF MAC       :     5c:f9:dd:ef:10:c9
Fabric Intf   :     Fc 0/0
FCoE Vlan     :     1003
Fabric Map    :     fid_1003
ENode WWPN    :     10:00:00:00:c9:d9:9c:cb
ENode WWNN    :     10:00:00:00:c9:d9:9c:cd
FCoE MAC      :     0e:fc:03:01:02:02
FC-ID         :     01:02:01
LoginMethod   :     FDISC
Secs          :     5593
Status        :     LOGGED_IN
```

Related Commands

dcb-map — creates a DCB map to configure DCB parameters on Ethernet ports that support converged Ethernet traffic.

fcoe-map — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

show fc switch

Display the switch configuration for Fibre Channel capability.

S5000

Syntax `show fc switch`

Parameters None

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `show interfaces fibrechannel` command to display information on the Fibre Channel capability of a switch.

The following table describes the `show fc switch` output shown in the following example.

Switch Mode	Fibre Channel mode of operation of an S5000 switch. Default: NPG (configured as an NPIV proxy gateway).
Switch WWN	Factory-assigned worldwide node (WWN) name of the S5000. The S5000 WWN name is not user-configurable.

Example

```
FTOS# show fc switch
Switch Mode : NPG
Switch WWN  : 10:00:5c:f9:dd:ef:10:c0
FTOS#
```

Related Commands

interface fibrechannel — configures a Fibre Channel interface on the switch.

show interfaces fibrechannel — displays the configuration of a Fibre Channel interface.

show qos dcb-map

Display the DCB parameters configured in a specified DCB map.

S5000

Syntax

`show qos dcb-map map-name`

Parameters

map-name	Displays the PFC and ETS parameters configured in the specified map.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `show qos dcb-map` command to display the enhanced transmission selection (ETS) and priority-based flow control (PFC) parameters used to configure server-facing Ethernet ports. S5000 Ethernet ports are DCBx-enabled by default.

The following table describes the `show qos dcb-map` output shown in the example below.

Field	Description
State	Complete: All mandatory DCB parameters are correctly configured. In progress: The DCB map configuration is not complete. Some mandatory parameters are not configured.
PFC Mode	PFC configuration in DCB map: On (enabled) or Off.
PG	Priority group configured in the DCB map.
TSA	Transmission scheduling algorithm used by the priority group: Enhanced Transmission Selection (ETS).
BW	Percentage of bandwidth allocated to the priority group.
PFC	PFC setting for the priority group: On (enabled) or Off.
Priorities	802.1p priorities configured in the priority group.

Example

```
FTOS# show qos dcb-map dcbmap2

State   :Complete
PfcMode:ON
--------------------
PG:0 TSA:ETS  BW:50  PFC:OFF
Priorities:0 1 2 4 5 6 7


PG:1 TSA:ETS  BW:50  PFC:ON
Priorities:3
```

Related Commands

dcb-map — creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports.

37

Open Shortest Path First (OSPFv2)

Open Shortest Path First (OSPFv2) is supported on the S5000 switch. Up to 16 OSPF instances can run simultaneously on the S5000.

OSPF is an interior gateway protocol (IGP), which means that it distributes routing information between routers in a single autonomous system (AS). OSPF is also a link-state protocol in which all routers contain forwarding tables derived from information about their links to their neighbors.

The Dell Networking implementation of OSPFv2 is based on IETF RFC 2328. The following commands allow you to configure and enable OSPFv2.

area default-cost

Set the metric for the summary default route generated by the area border router (ABR) into the stub area. Use this command on the border routers at the edge of a stub area.

S5000

Syntax

`area area-id default-cost cost`

To return default values, use the `no area area-id default-cost` command.

Parameters

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
cost	Specifies the stub area's advertised external route metric. The range is zero (0) to 65535.

Defaults

cost = 1; no areas are configured.

Command Modes

ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

In the Dell Networking operating software (FTOS), `cost` is defined as reference bandwidth/ bandwidth.

Related Commands

area stub – creates a stub area.

area nssa

Specify an area as a not so stubby area (NSSA).

S5000

Syntax	`area` *`area-id`* `nssa [default-information-originate] [no-redistribution] [no-summary]` To delete an NSSA, use the `no area area-id nssa` command.
Parameters	

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
default-information-originate	(OPTIONAL) Allows external routing information to be imported into the NSSA by using Type 7 default.
no-redistribution	(OPTIONAL) Specify that the `redistribute` command should not distribute routes into the NSSA. You should only use this command in a NSSA area border router (ABR).
no-summary	(OPTIONAL) Specify that no summary LSAs should be sent into the NSSA.

Defaults	Not configured.
Command Modes	ROUTER OSPF
Command History	

Version 9.0(1.3)	Introduced on the S5000.

area range

Summarize routes matching an address/mask at an area border router (ABR).

S5000

Syntax	`area` *`area-id`* `range` *`ip-address`* *`mask mask`* `[not-advertise]` To disable route summarization, use the `no area` *`area-id`* `range` *`ip-address mask`* command.
Parameters	

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
ip-address	Specify an IP address in dotted decimal format.
mask	Specify a mask for the destination prefix. Enter the full mask (for example, 255.255.255.0).

not-advertise	(OPTIONAL) Enter the keywords `not-advertise` to set the status to DoNotAdvertise (that is, the Type 3 summary-LSA is suppressed and the component networks remain hidden from other areas.)

Defaults Not configured.

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Only the routes within an area are summarized, and that summary is advertised to other areas by the ABR. External routes are not summarized.

Related Commands

area stub – creates a stub area.

router ospf – enters ROUTER OSPF mode to configure an OSPF instance.

area stub

Configure a stub area, which is an area not connected to other areas.

S5000

Syntax

```
area area-id stub [no-summary]
```

To delete a stub area, use the `no area area-id stub` command.

Parameters

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
no-summary	(OPTIONAL) Enter the keywords `no-summary` to prevent the ABR from sending summary Link State Advertisements (LSAs) into the stub area.

Defaults Disabled.

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Use this command to configure all routers and access servers within a stub.

Related Commands

router ospf – enters ROUTER OSPF mode to configure an OSPF instance.

area virtual-link

Set a virtual link and its parameters.

S5000

Syntax

```
area area-id virtual-link router-id [[authentication-key
[encryption-type] key] | [message-digest-key keyid md5
[encryption-type] key]] [dead-interval seconds] [hello-interval
seconds] [retransmit-interval seconds] [transmit-delay seconds]
```

To delete a virtual link, use the `no area area-id virtual-link router-id` command.

To delete a parameter of a virtual link, use the `no area area-id virtual-link router-id [[authentication-key [encryption-type] key] | [message-digest-key keyid md5 [encryption-type] key]] [dead-interval seconds] [hello-interval seconds] [retransmit-interval seconds] [transmit-delay seconds]` command syntax.

Parameters

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
router-id	Specify an ID (IP address in dotted decimal format) associated with a virtual link neighbor.
authentication-key [*encryption-type*] *key* | message-digest-key *keyid* md5 [*encryption-type*] *key*	(OPTIONAL) Choose between two authentication methods: • Enter the keywords `authentication-key` to enable simple authentication followed by an alphanumeric string up to eight characters long. Optionally, for the `encryption-type` variable, enter the number seven before entering the `key` string to indicate that an encrypted password will follow. • Enter the keywords `message-digest-key` followed by a number from 1 to 255 as the `keyid`. After the `keyid`, enter the keyword `md5` followed by the key. The key is an alphanumeric string up to 16 characters long. Optionally, for the `encryption-type` variable, enter the number seven before entering the `key` string to indicate that an encrypted password will follow.
dead-interval *seconds*	(OPTIONAL) Enter the keywords `dead-interval` followed by a number as the number of seconds for the interval. The range is 1 to 8192. The default is **40 seconds**.
hello-interval *seconds*	(OPTIONAL) Enter the keywords `hello-interval` followed by the number of seconds for the interval. The range is 1 to 8192. The default is **10 seconds**.
retransmit-interval *seconds*	(OPTIONAL) Enter the keywords `retransmit-interval` followed by the number of seconds for the interval. The range is 1 to 8192. The default is **5 seconds**.

transmit-delay ***seconds***	(OPTIONAL) Enter the keywords `transmit-delay` followed by the number of seconds for the interval. The range is 1 to 8192. The default is **1 second**.

Defaults

- dead-interval seconds = **40 seconds**
- hello-interval seconds = **10 seconds**
- retransmit-interval seconds = **5 seconds**
- transmit-delay seconds = **1 second**

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

All OSPF areas must be connected to a backbone area (usually Area 0). Virtual links connect broken or discontiguous areas.

You cannot enable both authentication options. Choose either the `authentication-key` or `message-digest-key` option.

Related Commands

router ospf – enters ROUTER OSPF mode to configure an OSPF instance.

auto-cost

Specify how the OSPF interface cost is calculated based on the reference bandwidth method.

S5000

Syntax

`auto-cost [reference-bandwidth ref-bw]`

To return to the default bandwidth or to assign cost based on the interface type, use the `no auto-cost [reference-bandwidth]` command.

Parameters

ref-bw	(OPTIONAL) Specify a reference bandwidth in megabits per second. The range is 1 to 4294967. The default is **100 megabits per second**.

Defaults **100 megabits per second.**

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ip ospf

Clear all OSPF routing tables.

S5000

Syntax

```
clear ip ospf process-id [process]
```

Parameters

process-id	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
process	(OPTIONAL) Enter the keyword `process` to reset the OSPF process.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ip ospf statistics

Clear the packet statistics in interfaces and neighbors.

S5000

Syntax

```
clear ip ospf process-id statistics [interface type slot/port
{neighbor router-id}]
```

Parameters

process-id	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
interface ***type slot/port***	(OPTIONAL) Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Null interface, enter the keywords `null 0`. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

neighbor *router-id*	(OPTIONAL) Enter the keyword `neighbor` followed by the neighbor's router-id in dotted decimal format (A.B.C.D.).

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands show ip ospf statistics – displays the OSPF statistics.

debug ip ospf

Display debug information on OSPF. Entering the `debug ip ospf` commands enables OSPF debugging for the first OSPF process.

S5000

Syntax

```
debug ip ospf process-id [bfd |event | packet | spf | database-
timer rate-limit]
```

To cancel the debug command, use the `no debug ip ospf` command.

Parameters

process-id	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
bfd	(OPTIONAL) Enter the keyword `bfd` to debug only OSPF BFD information.
event	(OPTIONAL) Enter the keyword `event` to debug only OSPF event information.
packet	(OPTIONAL) Enter the keyword `packet` to debug only OSPF packet information.
spf	(OPTIONAL) Enter the keyword `spf` to display the Shortest Path First information.
database-timer rate-limit	(OPTIONAL) Enter the keywords `database-timer rate-limit` to display the LSA throttling timer information.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The following describes output for the `debug ip ospf` command shown in the Example below.

Field	**Description**

8:14	Displays the time stamp.
OSPF	Displays the OSPF process ID: instance ID.
v:	Displays the OSPF version. FTOS supports version 2 only.
t:	Displays the type of packet sent: • 1 - Hello packet • 2 - database description • 3 - link state request • 4 - link state update • 5 - link state acknowledgement
l:	Displays the packet length.
rid:	Displays the OSPF router ID.
aid:	Displays the Autonomous System ID.
chk:	Displays the OSPF checksum.
aut:	States if OSPF authentication is configured. One of the following is listed: • 0 - no authentication configured • 1 - simple authentication configured using the `ip ospf authentication-key` command • 2 - MD5 authentication configured using the `ip ospf message-digest-key` command
auk:	If the `ip ospf authentication-key` command is configured, this field displays the key used.
keyid:	If the `ip ospf message-digest-key` command is configured, this field displays the MD5 key
to:	Displays the interface to which the packet is intended.
dst:	Displays the destination IP address.
netmask:	Displays the destination IP address mask.
pri:	Displays the OSPF priority
N, MC, E, T	Displays information available in the Options field of the HELLO packet: • N + (N-bit is set) • N - (N-bit is not set) • MC+ (bit used by MOSPF is set and router is able to forward IP multicast packets) • MC- (bit used by MOSPF is not set and router cannot forward IP multicast packets) • E + (router is able to accept AS External LSAs) • E - (router cannot accept AS External LSAs)

- T + (router can support TOS)
- T - (router cannot support TOS)

hi:	Displays the amount of time configured for the HELLO interval.
di:	Displays the amount of time configured for the DEAD interval.
dr:	Displays the IP address of the designated router.
bdr:	Displays the IP address of the Border Area Router.

Example

```
FTOS#debug ip ospf 1 packet
OSPF process 90, packet debugging is on

FTOS#
08:14:24 : OSPF(100:00):
Xmt. v:2 t:1(HELLO) l:44 rid:192.1.1.1
   aid:0.0.0.1 chk:0xa098 aut:0 auk: keyid:0 to:Te 4/3 dst:
224.0.0.5
      netmask:255.255.255.0 pri:1 N-, MC-, E+, T-,
      hi:10 di:40 dr:90.1.1.1 bdr:0.0.0.0
```

default-information originate

Configure the FTOS to generate a default external route into an OSPF routing domain.

S5000

Syntax

`default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]`

To return to the default values, use the `no default-information originate` command.

Parameters

always	(OPTIONAL) Enter the keyword `always` to specify that default route information must always be advertised.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` followed by a number to configure a metric value for the route. The range is 1 to 16777214.
metric-type *type-value*	(OPTIONAL) Enter the keywords `metric-type` followed by an OSPF link state type of 1 or 2 for default routes. The values are: • 1 = Type 1 external route • 2 = Type 2 external route
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of an established route map.

Defaults

Disabled.

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands redistribute – redistributes routes from other routing protocols into OSPF.

default-metric

Change the metrics of redistributed routes to a value useful to OSPF. Use this command with the `redistribute` command.

S5000

Syntax `default-metric` *`number`*

To return to the default values, use the `no default-metric [number]` command.

Parameters

number	Enter a number as the metric. The range is 1 to 16777214.

Defaults Disabled.

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands redistribute – redistributes routes from other routing protocols into OSPF.

description

Add a description about the selected OSPF configuration.

S5000

Syntax `description` *`description`*

To remove the OSPF description, use the `no description` command.

Parameters

description	Enter a text string description to identify the OSPF configuration (80 characters maximum).

Defaults none

Command Modes ROUTER OSPF

Command History	**Version 9.0(1.3)**	Introduced on the S5000.
Related Commands	show ip ospf asbr – displays the VLAN configuration.	

distance

Define an administrative distance for particular routes to a specific IP address.

S5000

Syntax

`distance` *`weight`* `[`*`ip-address mask access-list-name`*`]`

To delete the settings, use the `no distance weight [`*`ip-address mask access-list-name`*`]` command.

Parameters

weight	Specify an administrative distance. The range is 1 to 255. The default is **110**.
ip-address	(OPTIONAL) Enter a router ID in the dotted decimal format. If you enter a router ID, you must include the mask for that router address.
mask	(OPTIONAL) Enter a mask in dotted decimal format or /n format.
access-list-name	(OPTIONAL) Enter the name of an IP standard access list, up to 140 characters.

Defaults 110

Command Modes ROUTER OSPF

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

distance ospf

Configure an OSPF distance metric for different types of routes.

S5000

Syntax

`distance ospf [external` *`dist3`*`] [inter-area` *`dist2`*`] [intra-area` *`dist1`*`]`

To delete these settings, use the `no distance ospf` command.

Parameters

external ***dist3***	(OPTIONAL) Enter the keyword `external` followed by a number to specify a distance for external type 5 and 7 routes. The range is 1 to 255. The default is **110**.
inter-area ***dist2***	(OPTIONAL) Enter the keywords `inter-area` followed by a number to specify a distance metric for routes between areas. The range is 1 to 255. The default is **110**.
intra-area ***dist1***	(OPTIONAL) Enter the keywords `intra-area` followed by a number to specify a distance metric for all routes within an area. The range is 1 to 255. The default is **110**.

Defaults

- external *dist3* = **110**
- inter-area *dist2* = **110**
- intra-area *dist1* = **110**

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information To specify a distance for routes learned from other routing domains, use the `redistribute` command.

distribute-list in

Apply a filter to incoming routing updates from OSPF to the routing table.

S5000

Syntax `distribute-list` *`prefix-list-name`* `in [`*`interface-type slot/port`*`]`

To delete a filter, use the `no distribute-list` *`prefix-list-name`* `in [`*`interface-type slot/port`*`]` command.

Parameters

prefix-list-name **in**	Enter the name of a configured prefix list followed by the keyword `in`.
interface-type slot/port	(OPTIONAL) Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults Not configured.

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

distribute-list out

Apply a filter to restrict certain routes destined for the local routing table after the SPF calculation.

S5000

Syntax `distribute-list prefix-list-name out [bgp | connected | isis | static]`

To remove a filter, use the `no distribute-list prefix-list-name out [bgp | connected | isis | static]` command.

Parameters

***prefix-list-name* out**	Enter the name of a configured prefix list followed by the keyword `out`.
bgp	(OPTIONAL) Enter the keyword `bgp` to specify that BGP routes are distributed.
connected	(OPTIONAL) Enter the keyword `connected` to specify that connected routes are distributed.
isis	(OPTIONAL) Enter the keyword `isis` to specify that IS-IS routes are distributed.
static	(OPTIONAL) Enter the keyword `static` to specify that only manually configured routes are distributed.

Defaults Not configured.

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The `distribute-list out` command applies to routes being redistributed by autonomous system boundary routers (ASBRs) into OSPF. It can be applied to external type 2 and external type 1 routes, but not to intra-area and inter-area routes.

fast-convergence

This command sets the minimum LSA origination and arrival times to zero (0), allowing more rapid route computation so that convergence takes less time.

S5000

Syntax

`fast-convergence {number}`

To cancel fast-convergence, use the `no fast convergence` command.

Parameters

number	Enter the convergence level desired. The higher this parameter is set, the faster OSPF converge takes place. The range is 1 to 4.

Defaults

none.

Command Modes

ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The higher this parameter is set, the faster OSPF converge takes place.

NOTE: The faster the convergence, the more frequent the route calculations and updates. This impacts CPU utilization and may impact adjacency stability in larger topologies.

Generally, convergence level 1 meets most convergence requirements. Higher convergence levels should only be selected following consultation with Dell Networking technical support.

flood-2328

Enable RFC-2328 flooding behavior.

S5000

Syntax

`flood-2328`

To disable, use the `no flood-2328` command.

Defaults

Disabled.

Command Modes

ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

In OSPF, flooding is the most resource-consuming task. The flooding algorithm, described in RFC-2328, requires that OSPF flood LSAs (Link State Advertisements) on all interfaces, as governed by LSA's flooding scope (see Section 13 of the RFC). When multiple direct links connect two routers, the RFC-2328 flooding algorithm generates significant redundant information across all links.

By default, FTOS implements an enhanced flooding procedure that dynamically and intelligently determines when to optimize flooding. Whenever possible, the OSPF task attempts to reduce flooding overhead by selectively flooding on a subset of the interfaces between two routers.

When you enable `flood-2328`, this command configures FTOS to flood LSAs on all interfaces.

graceful-restart grace-period

Specifies the time duration, in seconds, that the router’s neighbors will continue to advertise the router as fully adjacent regardless of the synchronization state during a graceful restart.

S5000

Syntax

`graceful-restart grace-period` *`seconds`*

To disable the grace period, use the `no graceful-restart grace-period` command.

Parameters

seconds	Time duration, in seconds, that specifies the duration of the restart process before OSPF terminates the process. The range is 40 to 1800 seconds.

Defaults

Not Configured

Command Modes

ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

graceful-restart helper-reject

Specify the OSPF router to not act as a helper during graceful restart.

S5000

Syntax

`graceful-restart helper-reject` *`ip-address`*

To return to default value, use the `no graceful-restart helper-reject` command.

Parameters

ip-address	Enter the OSPF router-id, in IP address format, of the restart router that *will not* act as a helper during graceful restart.

Defaults

Not configured.

Command Modes

ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

graceful-restart mode

Enable the graceful restart mode.

S5000

Syntax `graceful-restart mode [planned-only | unplanned-only]`

To disable graceful restart mode, use the `no graceful-restart mode` command.

Parameters

planned-only	(OPTIONAL) Enter the keywords `planned-only` to indicate graceful restart is supported in a planned restart condition only.
unplanned-only	(OPTIONAL) Enter the keywords `unplanned-only` to indicate graceful restart is supported in an unplanned restart condition only.

Defaults Support for both planned and unplanned failures.

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

graceful-restart role

Specify the role for your OSPF router during graceful restart.

S5000

Syntax `graceful-restart role [helper-only | restart-only]`

To disable graceful restart role, use the `no graceful-restart role` command.

Parameters

role helper-only	(OPTIONAL) Enter the keywords `helper-only` to specify the OSPF router is a helper only during graceful restart.
role restart-only	(OPTIONAL) Enter the keywords `restart-only` to specify the OSPF router is a restart only during graceful-restart.

Defaults By default, OSPF routers are both helper and restart routers during a graceful restart.

Command Modes ROUTER OSPF

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

ip ospf auth-change-wait-time

OSPF provides a grace period while OSPF changes its interface authentication type. During the grace period, OSPF sends out packets with new and old authentication scheme untill the grace period expires.

S5000

Syntax `ip ospf auth-change-wait-time` *`seconds`*

To return to the default, use the `no ip ospf auth-change-wait-time` command.

Parameters

seconds	Enter the seconds. The range is 0 to 300.

Defaults zero (0) seconds.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip ospf authentication-key

Enable authentication and set an authentication key on OSPF traffic on an interface.

S5000

Syntax `ip ospf authentication-key [`*`encryption-type`*`]` *`key`*

To delete an authentication key, use the `no ip ospf authentication-key` command.

Parameters

encryption-type	(OPTIONAL) Enter 7 to encrypt the key.
key	Enter an eight-character string. Strings longer than eight characters are truncated.

Defaults Not configured.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	All neighboring routers in the same network must use the same password to exchange OSPF information.

ip ospf cost

Change the cost associated with the OSPF traffic on an interface.

S5000

Syntax

`ip ospf cost cost`

To return to default value, use the `no ip ospf cost` command.

Parameters

cost	Enter a number as the cost. The range is 1 to 65535.

Defaults The default cost is based on the reference bandwidth.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If this command is not configured, cost is based on the `auto-cost` command.

When you configure OSPF over multiple vendors, use the `ip ospf cost` command to ensure that all routers use the same cost. Otherwise, OSPF routes improperly.

Related Commands auto-cost – controls how the OSPF interface cost is calculated.

ip ospf dead-interval

Set the time interval since the last hello-packet was received from a router. After the interval elapses, the neighboring routers declare the router dead.

S5000

Syntax

`ip ospf dead-interval seconds`

To return to the default values, use the `no ip ospf dead-interval` command.

Parameters

seconds	Enter the number of seconds for the interval. The range is 1 to 65535. The default is **40 seconds**.

Defaults **40 seconds**

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

By default, the dead interval is four times the default hello-interval.

Related Commands

ip ospf hello-interval – sets the time interval between the hello packets.

ip ospf hello-interval

Specify the time interval between the hello packets sent on the interface.

S5000

Syntax

```
ip ospf hello-interval seconds
```

To return to the default value, use the `no ip ospf hello-interval` command.

Parameters

seconds	Enter the number of seconds for the interval. The range is 1 to 65535. The default is **10 seconds**.

Defaults

10 seconds

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The time interval between the hello packets must be the same for routers in a network.

Related Commands

ip ospf dead-interval – sets the time interval before a router is declared dead.

ip ospf message-digest-key

Enable OSPF MD5 authentication and send an OSPF message digest key on the interface.

S5000

Syntax

```
ip ospf message-digest-key keyid md5 key
```

To delete a key, use the `no ip ospf message-digest-key keyid` command.

Parameters

keyid	Enter a number as the key ID. The range is 1 to 255.

key	Enter a continuous character string as the password.

Defaults No MD5 authentication is configured.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To change to a different key on the interface, enable the new key while the old key is still enabled. The FTOS sends two packets: the first packet authenticated with the old key and the second packet authenticated with the new key. This process ensures that the neighbors learn the new key and communication is not disrupted by keeping the old key enabled.

After the reply is received and the new key is authenticated, you must delete the old key. Dell Networking recommends keeping only one key per interface.

NOTE: The MD5 secret is stored as plain text in the configuration file with service password encryption.

ip ospf mtu-ignore

Disable OSPF MTU mismatch detection upon receipt of database description (DBD) packets.

S5000

Syntax

```
ip ospf mtu-ignore
```

To return to the default, use the `no ip ospf mtu-ignore` command.

Defaults Enabled.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip ospf network

Set the network type for the interface.

S5000

Syntax

```
ip ospf network {broadcast | point-to-point}
```

To return to the default, use the `no ip ospf network` command.

Parameters

broadcast	Enter the keyword `broadcast` to designate the interface as part of a broadcast network.

point-to-point	Enter the keywords `point-to-point` to designate the interface as part of a point-to-point network.

Defaults Not configured.

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip ospf priority

Set the priority of the interface to determine the designated router for the OSPF network.

S5000

Syntax `ip ospf priority` *`number`*

To return to the default setting, use the `no ip ospf priority` command.

Parameters

number	Enter a number as the priority. The range is 0 to 255. The default is **1**.

Defaults **1**

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Setting a priority of 0 makes the router ineligible for election as a designated router or backup designated router.

Use this command for interfaces connected to multi-access networks, not point-to-point networks.

ip ospf retransmit-interval

Set the retransmission time between lost link state advertisements (LSAs) for adjacencies belonging to the interface.

S5000

Syntax `ip ospf retransmit-interval` *`seconds`*

To return to the default values, use the `no ip ospf retransmit-interval` command.

Parameters

seconds	Enter the number of seconds as the interval between retransmission. The range is 1 to 3600. The default is **5 seconds**.

	This interval must be greater than the expected round-trip time for a packet to travel between two routers.

Defaults	**5 seconds**
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Set the time interval to a number large enough to prevent unnecessary retransmissions. For example, the interval should be larger for interfaces connected to virtual links.

ip ospf transmit-delay

Set the estimated time elapsed to send a link state update packet on the interface.

S5000

Syntax

`ip ospf transmit-delay *seconds*`

To return to the default value, use the `no ip ospf transmit-delay` command.

Parameters

seconds	Enter the number of seconds as the interval between retransmission. The range is 1 to 3600. The default is **1 second**. This value must be greater than the transmission and propagation delays for the interface.

Defaults	**1 second**
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

log-adjacency-changes

Set FTOS to send a Syslog message about changes in the OSPF adjacency state.

S5000

Syntax

`log-adjacency-changes`

To disable the Syslog messages, use the `no log-adjacency-changes` command.

Defaults Disabled.

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

maximum-paths

Enable the software to forward packets over multiple paths.

S5000

Syntax `maximum-paths *number*`

To disable packet forwarding over multiple paths, use the `no maximum-paths` command.

Parameters

number	Specify the number of paths. The range is 1 to 16. The default is **4 paths**.

Defaults **4**

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

mib-binding

Enable this OSPF process ID to manage the SNMP traps and process SNMP queries.

S5000

Syntax `mib-binding`

To mib-binding on this OSPF process, use the `no mib-binding` command.

Defaults none.

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command is either enabled or disabled. If no OSPF process is identified as the MIB manager, the first OSPF process is used.

If an OSPF process has been selected, it must be disabled prior to assigning new process ID the MIB responsibility.

network area

Define which interfaces run OSPF and the OSPF area for those interfaces.

S5000

Syntax

`network ip-address mask area area-id`

To disable an OSPF area, use the `no network ip-address mask area area-id` command.

Parameters

ip-address	Specify a primary or secondary address in dotted decimal format. The primary address is required before adding the secondary address.
mask	Enter a network mask in /prefix format. (/x)
area-id	Enter the OSPF area ID as either a decimal value or in a valid IP address. Decimal value range is 0 to 65535. IP address format is dotted decimal format A.B.C.D. **NOTE:** If the area ID is smaller than 65535, it is converted to a decimal value. For example, if you use an area ID of 0.0.0.1, it is converted to 1.

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To enable OSPF on an interface, the `network area` command must include, in its range of addresses, the primary IP address of an interface.

NOTE: An interface can be attached only to a single OSPF area.

If you delete all the network area commands for Area 0, the `show ip ospf` command output will not list Area 0.

passive-interface

Suppress both receiving and sending routing updates on an interface.

S5000

Syntax

`passive-interface {default | interface}`

To enable both the receiving and sending routing, use the `no passive-interface interface` command.

To return all OSPF interfaces (current and future) to active, use the `no passive-interface default` command.

Parameters

default	Enter the keyword `default` to make all OSPF interfaces (current and future) passive.
interface	Enter the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information. • For Port Channel groups, enter the keywords `port-channel` followed by a number. The range is 1 to 128. • For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Although the passive interface will neither send nor receive routing updates, the network on that interface will still be included in OSPF updates sent using other interfaces.

The `default` keyword sets all interfaces as passive. You can then configure individual interfaces, where adjacencies are desired, using the `no passive-interface` *`interface`* command. The `no` form of this command is inserted into the configuration for individual interfaces when the `no passive-interface` *`interface`* command is issued while `passive-interface default` is configured.

This command behavior has changed as follows:

`passive-interface` *`interface`*

- The previous `no passive-interface` *`interface`* is removed from the running configuration.
- The ABR status for the router is updated.
- Save `passive-interface` *`interface`* into the running configuration.

`passive-interface default`

- All present and future OSPF interface are marked as *passive*.
- Any adjacency are explicitly terminated from all OSPF interfaces.
- All previous `passive-interface` *`interface`* commands are removed from the running configuration.
- All previous `no passive-interface` *`interface`* commands are removed from the running configuration.

`no passive-interface` *`interface`*

- Remove the interface from the passive list.
- The ABR status for the router is updated.

- If `passive-interface default` is specified, then save `no passive-interface` *`interface`* into the running configuration.

`No passive-interface default`

- Clear everything and revert to the default behavior.
- All previously marked passive interfaces are removed.
- May update ABR status.

debug ip ospf

Display debug information on OSPF. Entering the `debug ip ospf` commands enables OSPF debugging for the first OSPF process.

S5000

Syntax

```
debug ip ospf process-id [bfd |event | packet | spf | database-
timer rate-limit]
```

To cancel the debug command, use the `no debug ip ospf` command.

Parameters

process-id	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
bfd	(OPTIONAL) Enter the keyword `bfd` to debug only OSPF BFD information.
event	(OPTIONAL) Enter the keyword `event` to debug only OSPF event information.
packet	(OPTIONAL) Enter the keyword `packet` to debug only OSPF packet information.
spf	(OPTIONAL) Enter the keyword `spf` to display the Shortest Path First information.
database-timer rate-limit	(OPTIONAL) Enter the keywords `database-timer rate-limit` to display the LSA throttling timer information.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output for the `debug ip ospf` command shown in the Example below.

Field	Description
8:14	Displays the time stamp.
OSPF	Displays the OSPF process ID: instance ID.

v:	Displays the OSPF version. FTOS supports version 2 only.
t:	Displays the type of packet sent: • 1 - Hello packet • 2 - database description • 3 - link state request • 4 - link state update • 5 - link state acknowledgement
l:	Displays the packet length.
rid:	Displays the OSPF router ID.
aid:	Displays the Autonomous System ID.
chk:	Displays the OSPF checksum.
aut:	States if OSPF authentication is configured. One of the following is listed: • 0 - no authentication configured • 1 - simple authentication configured using the `ip ospf authentication-key` command • 2 - MD5 authentication configured using the `ip ospf message-digest-key` command
auk:	If the `ip ospf authentication-key` command is configured, this field displays the key used.
keyid:	If the `ip ospf message-digest-key` command is configured, this field displays the MD5 key
to:	Displays the interface to which the packet is intended.
dst:	Displays the destination IP address.
netmask:	Displays the destination IP address mask.
pri:	Displays the OSPF priority
N, MC, E, T	Displays information available in the Options field of the HELLO packet: • N + (N-bit is set) • N - (N-bit is not set) • MC+ (bit used by MOSPF is set and router is able to forward IP multicast packets) • MC- (bit used by MOSPF is not set and router cannot forward IP multicast packets) • E + (router is able to accept AS External LSAs) • E - (router cannot accept AS External LSAs) • T + (router can support TOS) • T - (router cannot support TOS)

hi:	Displays the amount of time configured for the HELLO interval.
di:	Displays the amount of time configured for the DEAD interval.
dr:	Displays the IP address of the designated router.
bdr:	Displays the IP address of the Border Area Router.

Example

```
FTOS#debug ip ospf 1 packet
OSPF process 90, packet debugging is on

FTOS#
08:14:24 : OSPF(100:00):
Xmt. v:2 t:1(HELLO) l:44 rid:192.1.1.1
   aid:0.0.0.1 chk:0xa098 aut:0 auk: keyid:0 to:Te 4/3 dst:
224.0.0.5
      netmask:255.255.255.0 pri:1 N-, MC-, E+, T-,
      hi:10 di:40 dr:90.1.1.1 bdr:0.0.0.0
```

redistribute bgp

Redistribute BGP routing information throughout the OSPF instance.

S5000

Syntax

`redistribute bgp as` *`number`* `[metric` *`metric-value`*`] | [metric-type` *`type-value`*`] | [tag` *`tag-value`*`]`

To disable redistribution, use the `no redistribute bgp as` *`number`* `[metric` *`metric-value`*`] | [metric-type` *`type-value`*`] [route-map` *`map-name`*`] [tag` *`tag-value`*`]` command.

Parameters

as number	Enter the autonomous system number. The range is 1 to 65535.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` followed by the metric-value number. The range is 0 to16777214.
metric-type *type-value*	(OPTIONAL) Enter the keywords `metric-type` followed by one of the following: • 1 = for OSPF External type 1 • 2 = for OSPF External type 2
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of the route map.
tag *tag-value*	(OPTIONAL) Enter the keyword `tag` to set the tag for routes redistributed into OSPF. The range is 0 to 4294967295.

Defaults none

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

redistribute isis

Redistribute IS-IS routing information throughout the OSPF instance.

S5000

Syntax

`redistribute isis [`*`tag`*`] [level-1 | level-1-2 | level-2] [metric `*`metric-value`*` | metric-type `*`type-value`*`] [route-map `*`map-name`*`] [tag `*`tag-value`*`]`

To disable redistribution, use the `no redistribute isis [`*`tag`*`] [level-1 | level-1-2 | level-2] [metric `*`metric-value`*` | metric-type `*`type-value`*`] [route-map `*`map-name`*`] [tag `*`tag-value`*`]` command.

Parameters

tag	(OPTIONAL) Enter the name of the IS-IS routing process.
level-1	(OPTIONAL) Enter the keywords `level-1` to redistribute only IS-IS Level-1 routes.
level-1-2	(OPTIONAL) Enter the keywords `level-1-2` to redistribute both IS-IS Level-1 and Level-2 routes.
level-2	(OPTIONAL) Enter the keywords `level-2` to redistribute only IS-IS Level-2 routes.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` followed by a number. The range is 0 (zero) to 4294967295.
metric-type *type-value*	(OPTIONAL) Enter the keywords `metric-type` followed by one of the following: • 1 = for OSPF External type 1 • 2 = for OSPF External type 2
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of the route map.
tag *tag-value*	(OPTIONAL) Enter the keyword `tag` to set the tag for routes redistributed into OSPF. The range is 0 to 4294967295.

Defaults Not configured.

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

router-id

Use this command to configure a fixed router ID.

S5000

Syntax

`router-id ip-address`

To remove the fixed router ID, use the `no router-id ip-address` command.

Parameters

ip-address	Enter the router ID in the IP address format.

Defaults none.

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique. If you use this command on an OSPF router process, which is already active (that is, has neighbors), a prompt reminding you that changing the router-id brings down the existing OSPF adjacency. The new router ID is effective at the next reload.

Example

```
FTOS(conf)#router ospf 100
FTOS(conf-router_ospf)#router-id 1.1.1.1
Changing router-id will bring down existing OSPF adjacency [y/
n]:

FTOS(conf-router_ospf)#show config
!
router ospf 100
router-id 1.1.1.1
FTOS(conf-router_ospf)#no router-id
Changing router-id will bring down existing OSPF adjacency [y/
n]:
FTOS#
```

router ospf

Enter ROUTER OSPF mode to configure an OSPF instance.

S5000

Syntax

`router ospf process-id`

To clear an OSPF instance, use the `no router ospf process-id` command.

Parameters

process-id	Enter a number for the OSPF instance. The range is 1 to 65535.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must have an IP address assigned to an interface to enter ROUTER OSPF mode and configure OSPF.

After the OSPF process and the VRF are tied together, you cannot use the OSPF Process ID again in the system.

Example

```
FTOS(conf)#router ospf 2
FTOS(conf-router_ospf)#
```

show config

Display the non-default values in the current OSPF configuration.

S5000

Syntax `show config`

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-router_ospf)#show config
!
router ospf 3
passive-interface tengigabitethernet 0/1
FTOS(conf-router_ospf)#
```

show ip ospf

Display information on the OSPF process configured on the switch.

S5000

Syntax `show ip ospf` *`process-id`*

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Command Modes

- EXEC

- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you delete all the network area commands for Area 0, the `show ip ospf` command output does not list Area 0.

The following describes the output from the `show ip ospf` command shown in the Example below.

Line Beginning with	Description
Routing Process...	Displays the OSPF process ID and the IP address associated with the process ID.
Supports only...	Displays the number of Type of Service (TOS) rouse supported.
SPF schedule...	Displays the delay and hold time configured for this process ID.
Convergence Level	
Min LSA....	Displays the intervals set for LSA transmission and acceptance.
Number of...	Displays the number and type of areas configured for this process ID.

Example

```
FTOS#show ip ospf 10
Routing Process ospf 10 with ID 1.1.1.1 Virtual router default-
vrf
Supports only single TOS (TOS0) routes
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Convergence Level 0
Min LSA origination 0 msec, Min LSA arrival 1000 msec
Min LSA hold time 5000 msec, Max LSA wait time 5000 msec
Number of area in this router is 1, normal 1 stub 0 nssa 0
    Area BACKBONE (0)
      Number of interface in this area is 1
      SPF algorithm executed 205 times
      Area ranges are
FTOS#
```

Related Commands

show ip ospf database – displays information about the OSPF routes configured.

show ip ospf interface – displays the OSPF interfaces configured.

show ip ospf neighbor – displays the OSPF neighbors configured.

show ip ospf virtual-links – displays the OSPF virtual links configured.

show ip ospf asbr

Display all autonomous system boundary routers (ASBR) visible to OSPF.

S5000

Syntax	`show ip ospf process-id asbr`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use this command to isolate problems with external routes. In OSPF, external routes are calculated by adding the LSA cost to the cost of reaching the ASBR router. If an external route does not have the correct cost, use this command to determine if the path to the originating router is correct. The display output is not sorted in any order.

NOTE: ASBRs that are not in directly connected areas are also displayed.

You can determine if an ASBR is in a directly connected area (or not) by the flags. For ASBRs in a directly connected area, E flags are set. In the Example below, router 1.1.1.1 is in a directly connected area since the Flag is E/-/-/. For remote ASBRs, the E flag is clear (-/-/-/).

Example

```
FTOS#show ip ospf 1asbr

RouterID  Flags   Cost Nexthop   Interface Area
3.3.3.3   -/-/-/  2   10.0.0.2   Te 0/1    1
1.1.1.1   E/-/-/  0   0.0.0.0    -         0
FTOS#
```

show ip ospf database

Display all LSA information. If you do not enable OSPF on the switch, no output is generated.

S5000

Syntax	`show ip ospf process-id database [database-summary]`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

database-summary	(OPTIONAL) Enter the keywords `database-summary` to the display the number of LSA types in each area and the total number of LSAs.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output for the `show ip ospf` *`process-id`* `database` command shown in the Example below.

Field	Description
Link ID	Identifies the router ID.
ADV Router	Identifies the advertising router's ID.
Age	Displays the link state age.
Seq#	Identifies the link state sequence number. This number allows you to identify old or duplicate link state advertisements.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.
Link count	Displays the number of interfaces for that router.

Example

```
FTOS>show ip ospf 1 database

     OSPF Router with ID (11.1.2.1) (Process ID 1)
                Router (Area 0.0.0.0)
Link ID      ADV Router   Age  Seq#       Checksum Link count
11.1.2.1     11.1.2.1     673  0x80000005 0x707e   2
13.1.1.1     13.1.1.1     676  0x80000097 0x1035   2
192.68.135.2 192.68.135.2 1419 0x80000294 0x9cbd   1

               Network (Area 0.0.0.0)
Link ID      ADV Router   Age  Seq#       Checksum
10.2.3.2     13.1.1.1     676  0x80000003 0x6592
10.2.4.2     192.68.135.2 908  0x80000055 0x683e

               Type-5 AS External
Link ID      ADV Router   Age  Seq#       Checksum Tag
0.0.0.0      192.68.135.2 908  0x80000052 0xeb83   100
1.1.1.1      192.68.135.2 908  0x8000002a 0xbd27   0
10.1.1.0     11.1.2.1     718  0x80000002 0x9012   0
10.1.2.0     11.1.2.1     718  0x80000002 0x851c   0
10.2.2.0     11.1.2.1     718  0x80000002 0x7927   0
10.2.3.0     11.1.2.1     718  0x80000002 0x6e31   0
10.2.4.0     13.1.1.1     1184 0x80000068 0x45db   0
11.1.1.0     11.1.2.1     718  0x80000002 0x831e   0
11.1.2.0     11.1.2.1     718  0x80000002 0x7828   0
12.1.2.0     192.68.135.2 1663 0x80000054 0xd8d6   0
13.1.1.0     13.1.1.1     1192 0x8000006b 0x2718   0
13.1.2.0     13.1.1.1     1184 0x8000006b 0x1c22   0
172.16.1.0   13.1.1.1     148  0x8000006d 0x533b   0
FTOS>
```

Related Commands

show ip ospf database asbr-summary – displays only ASBR summary LSA information.

show ip ospf database asbr-summary

Display information about autonomous system (AS) boundary LSAs.

S5000

Syntax

`show ip ospf process-id database asbr-summary [link-state-id] [adv-router ip-address]`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output from the `show ip ospf database asbr-summary` command shown in the Example below.

LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.

Link State ID	Displays the Link State ID.
Advertising Router	Identifies the advertising router's ID.
Checksum	Displays the Fletcher checksum of the an LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Network Mask	Displays the network mask implemented on the area.
TOS	Displays the Type of Service (TOS) options. Option 0 is the only option.
Metric	Displays the LSA metric.

Example

```
FTOS#show ip ospf 100 database asbr-summary

     OSPF Router with ID (1.1.1.10) (Process ID 100)

       Summary Asbr (Area 0.0.0.0)

LS age: 1437
Options: (No TOS-capability, No DC, E)
LS type: Summary Asbr
Link State ID: 103.1.50.1
Advertising Router: 1.1.1.10
LS Seq Number: 0x8000000f
Checksum: 0x8221
Length: 28
Network Mask: /0
      TOS: 0 Metric: 2

LS age: 473
Options: (No TOS-capability, No DC, E)
LS type: Summary Asbr
Link State ID: 104.1.50.1
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000010
Checksum: 0x4198
Length: 28
--More--
```

Related Commands

show ip ospf database – displays OSPF database information.

show ip ospf database external

Display information on the AS external (type 5) LSAs.

S5000

Syntax

```
show ip ospf process-id database external [link-state-id] [adv-
router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output from the `show ip ospf` *`process-id`* `database external` command shown in the Example below.

LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
LS Seq Number	Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.
Checksum	Displays the Fletcher checksum of the an LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Network Mask	Displays the network mask implemented on the area.
Metrics Type	Displays the external type.
TOS	Displays the Type of Service (TOS) options. Option 0 is the only option.
Metric	Displays the LSA metric.
Forward Address	Identifies the address of the forwarding router. Data traffic is forwarded to this router. If the forwarding address is 0.0.0.0, data traffic is forwarded to the originating router.

External Route Tag	Displays the 32-bit field attached to each external route. This field is not used by the OSPF protocol, but can be used for external route management.

Example

```
FTOS#show ip ospf 1 database external

    OSPF Router with ID (20.20.20.5) (Process ID 1)

         Type-5 AS External

LS age: 612
Options: (No TOS-capability, No DC, E)
LS type: Type-5 AS External
Link State ID: 12.12.12.2
Advertising Router: 20.31.3.1
LS Seq Number: 0x80000007
Checksum: 0x4cde
Length: 36
Network Mask: /32
     Metrics Type: 2
     TOS: 0
     Metrics: 25
     Forward Address: 0.0.0.0
     External Route Tag: 43

LS age: 1868
Options: (No TOS-capability, DC)
LS type: Type-5 AS External
Link State ID: 24.216.12.0
Advertising Router: 20.20.20.8
LS Seq Number: 0x80000005
Checksum: 0xa00e
Length: 36
Network Mask: /24
     Metrics Type: 2
     TOS: 0
     Metrics: 1
     Forward Address: 0.0.0.0
     External Route Tag: 701
FTOS#
```

Related Commands

show ip ospf database – displays OSPF database information.

show ip ospf database network

Display the network (type 2) LSA information.

S5000

Syntax

show ip ospf *process-id* database network [*link-state-id*] [adv-router *ip-address*]

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router ***ip-address***	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output from the `show ip ospf` *`process-id`* `database network` command shown in the Example below.

LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
Checksum	Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.
Length	Displays the Fletcher checksum of an LSA's complete contents.
Network Mask	Displays the length in bytes of the LSA.
Attached Router	Identifies the IP address of routers attached to the network.

Example

```
FTOS#show ip ospf 1 data network

    OSPF Router with ID (20.20.20.5) (Process ID 1)

        Network (Area 0.0.0.0)
 LS age: 1372
Options: (No TOS-capability, DC, E)
LS type: Network
```

```
Link State ID: 202.10.10.2
Advertising Router: 20.20.20.8
LS Seq Number: 0x80000006
Checksum: 0xa35
Length: 36
Network Mask: /24
     Attached Router: 20.20.20.8
     Attached Router: 20.20.20.9
     Attached Router: 20.20.20.7

         Network (Area 0.0.0.1)

LS age: 252
Options: (TOS-capability, No DC, E)
LS type: Network
Link State ID: 192.10.10.2
Advertising Router: 192.10.10.2
LS Seq Number: 0x80000007
Checksum: 0x4309
Length: 36
Network Mask: /24
     Attached Router: 192.10.10.2
     Attached Router: 20.20.20.1
     Attached Router: 20.20.20.5
FTOS#
```

Related Commands

show ip ospf database – displays OSPF database information.

show ip ospf database nssa-external

Display NSSA-External (type 7) LSA information.

S5000

Syntax

`show ip ospf database nssa-external [link-state-id] [adv-router ip-address]`

Parameters

link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

show ip ospf database – displays OSPF database information.

show ip ospf database opaque-area

Display the opaque-area (type 10) LSA information.

S5000

Syntax

```
show ip ospf process-id database opaque-area [link-state-id]
[adv-router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output from the `show ip ospf process-id database opaque-area` command shown in the Example below.

LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.

LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the advertising router's ID.
Checksum	Displays the Fletcher checksum of the an LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Opaque Type	Displays the Opaque type field (the first 8 bits of the Link State ID).
Opaque ID	Displays the Opaque type-specific ID (the remaining 24 bits of the Link State ID).

Example

```
FTOS>show ip ospf 1 database opaque-area

    OSPF Router with ID (3.3.3.3) (Process ID 1)
         Type-10 Opaque Link Area (Area 0)

LS age: 1133
Options: (No TOS-capability, No DC, E)
LS type: Type-10 Opaque Link Area
Link State ID: 1.0.0.1
Advertising Router: 10.16.1.160
LS Seq Number: 0x80000416
Checksum: 0x376
Length: 28
Opaque Type: 1
Opaque ID: 1
Unable to display opaque data

LS age: 833
Options: (No TOS-capability, No DC, E)
LS type: Type-10 Opaque Link Area
Link State ID: 1.0.0.2
Advertising Router: 10.16.1.160
LS Seq Number: 0x80000002
Checksum: 0x19c2
--More--
```

Related Commands

show ip ospf database – displays OSPF database information.

show ip ospf database opaque-as

Display the opaque-as (type 11) LSA information.

S5000

Syntax

```
show ip ospf process-id database opaque-as [link-state-id]
[adv-router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

show ip ospf database – displays OSPF database information.

show ip ospf database opaque-link

Display the opaque-link (type 9) LSA information.

S5000

Syntax

```
show ip ospf process-id database opaque-link [link-state-id]
[adv-router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` followed by the IP address of an Advertising Router to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

show ip ospf database – displays OSPF database information.

show ip ospf database router

Display the router (type 1) LSA information.

S5000

Syntax

```
show ip ospf process-id database router [link-state-id] [adv-
router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` followed by the IP address of an Advertising Router to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output for the `show ip ospf process-id database router` command shown in the Example below.

LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.

- DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.
- E or No E is displayed on whether the originating router can accept AS External LSAs.

LS Type	Displays the LSA type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
LS Seq Number	Displays the link state sequence number. This number detects duplicate or old LSAs.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Number of Links	Displays the number of active links to the type of router (Area Border Router or AS Boundary Router) listed in the previous line.
Link connected to:	Identifies the type of network to which the router is connected.
(Link ID)	Identifies the link type and address.
(Link Data)	Identifies the router interface address.
Number of TOS Metric	Lists the number of TOS metrics.
TOS 0 Metric	Lists the number of TOS 0 metrics.

Example

```
FTOS#show ip ospf 100 database router

     OSPF Router with ID (1.1.1.10) (Process ID 100)

         Router (Area 0)

LS age: 967
Options: (No TOS-capability, No DC, E)
LS type: Router
Link State ID: 1.1.1.10
Advertising Router: 1.1.1.10
LS Seq Number: 0x8000012f
Checksum: 0x3357
Length: 144
AS Boundary Router
Area Border Router
  Number of Links: 10

  Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.129.1
    (Link Data) Router Interface address: 192.68.129.1
    Number of TOS metric: 0
       TOS 0 Metric: 1

  Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.130.1
    (Link Data) Router Interface address: 192.68.130.1
    Number of TOS metric: 0
```

```
        TOS 0 Metric: 1

   Link connected to: a Transit Network
     (Link ID) Designated Router address: 192.68.142.2
     (Link Data) Router Interface address: 192.68.142.2
     Number of TOS metric: 0
        TOS 0 Metric: 1

   Link connected to: a Transit Network
     (Link ID) Designated Router address: 192.68.141.2
     (Link Data) Router Interface address: 192.68.141.2
     Number of TOS metric: 0
        TOS 0 Metric: 1

   Link connected to: a Transit Network
     (Link ID) Designated Router address: 192.68.140.2
     (Link Data) Router Interface address: 192.68.140.2
     Number of TOS metric: 0
        TOS 0 Metric: 1

 Link connected to: a Stub Network
     (Link ID) Network/subnet number: 11.1.5.0
--More--
```

Related Commands show ip ospf database – displays OSPF database information.

show ip ospf database summary

Display the network summary (type 3) LSA routing information.

S5000

Syntax `show ip ospf process-id database summary [link-state-id] [adv-router ip-address]`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` followed by the IP address of an Advertising Router to display only the LSA information about that router.

Command Modes

- EXEC

- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output for the `show ip ospf` *`process-id`* `database summary` command shown in the Example below.

LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
LS Seq Number	Displays the link state sequence number. This number allows you to identify old or duplicate LSAs.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Network Mask	Displays the network mask implemented on the area.
TOS	Displays the TOS options. Option 0 is the only option.
Metric	Displays the LSA metrics.

Example

```
FTOS#show ip ospf 100 database summary

    OSPF Router with ID (1.1.1.10) (Process ID 100)

        Summary Network (Area 0.0.0.0)

LS age: 1551
Options: (No TOS-capability, DC, E)
LS type: Summary Network
Link State ID: 192.68.16.0
Advertising Router: 192.168.17.1
LS Seq Number: 0x80000054
Checksum: 0xb5a2
Length: 28
Network Mask: /24
    TOS: 0 Metric: 1

LS age: 9
Options: (No TOS-capability, No DC, E)
LS type: Summary Network
```

```
Link State ID: 192.68.32.0
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000016
Checksum: 0x987c
Length: 28
Network Mask: /24
   TOS: 0 Metric: 1

LS age: 7
Options: (No TOS-capability, No DC, E)
LS type: Summary Network
Link State ID: 192.68.33.0
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000016
Checksum: 0x1241
Length: 28
Network Mask: /26
   TOS: 0 Metric: 1

FTOS#
```

Related Commands show ip ospf database – displays OSPF database information.

show ip ospf interface

Display the OSPF interfaces configured. If OSPF is not enabled on the switch, no output is generated.

S5000

Syntax `show ip ospf process-id interface [type slot/port]`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
interface *type slot/port*	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Null interface, enter the keywords `null 0`. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output for the `show ip ospf` *`process-id`* `interface` command shown in the Example below.

Line beginning with	Description
TenGigabitEthernet...	This line identifies the interface type slot/port and the status of the OSPF protocol on that interface.
Internet Address...	This line displays the IP address, network mask and area assigned to this interface.
Process ID...	This line displays the OSPF Process ID, Router ID, Network type and cost metric for this interface.
Transmit Delay...	This line displays the interface's settings for Transmit Delay, State, and Priority. In the State setting, BDR is Backup Designated Router.
Designated Router...	This line displays the ID of the Designated Router and its interface address.
Backup Designated...	This line displays the ID of the Backup Designated Router and its interface address.
Timer intervals...	This line displays the interface's timer settings for Hello interval, Dead interval, Transmit Delay (Wait), and Retransmit Interval.
Hello due...	This line displays the amount time untill the next Hello packet is sent out this interface.
Neighbor Count...	This line displays the number of neighbors and adjacent neighbors. Listed below this line are the details about each adjacent neighbor.

Example

```
FTOS>show ip ospf int

TenGigabitEthernet 13/17 is up, line protocol is up
  Internet Address 192.168.1.2/30, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.253.2, Interface address
192.168.1.2
  Backup Designated Router (ID) 192.168.253.1, Interface
address 192.168.1.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:02
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.253.1 (Backup Designated
Router)

TenGigabitEthernet 13/23 is up, line protocol is up
  Internet Address 192.168.0.1/24, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.253.5, Interface address
192.168.0.4
  Backup Designated Router (ID) 192.168.253.3, Interface
address 192.168.0.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:08
  Neighbor Count is 3, Adjacent neighbor count is 2
    Adjacent with neighbor 192.168.253.5 (Designated Router)
    Adjacent with neighbor 192.168.253.3 (Backup Designated
Router)

Loopback 0 is up, line protocol is up
  Internet Address 192.168.253.2/32, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type
LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host.
FTOS>
```

show ip ospf neighbor

Display the OSPF neighbors connected to the local router.

S5000

Syntax `show ip ospf process-id neighbor`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The following describes output for the `show ip ospf process-id neighbor` command shown in the Example below.

Neighbor ID	Displays the neighbor router ID.
Pri	Displays the priority assigned neighbor.
State	Displays the OSPF state of the neighbor.
Dead Time	Displays the expected time until FTOS declares the neighbor dead.
Address	Displays the IP address of the neighbor.
Interface	Displays the interface type slot/port information.
Area	Displays the neighbor’s area (process ID).

Example

```
FTOS#show ip ospf 34 neighbor

Neighbor ID Pri State       Dead Time Address  Interface Area
20.20.20.7  1 FULL/DR     00:00:32 182.10.10.3 Te 0/0 0.0.0.2
192.10.10.2 1 FULL/DR     00:00:37 192.10.10.2 Te 0/1 0.0.0.1
20.20.20.1  1 FULL/DROTHER00:00:36 192.10.10.4 Te 0/1 0.0.0.1
FTOS#
```

show ip ospf routes

Display routes as calculated by OSPF and stored in OSPF RIB.

S5000

Syntax `show ip ospf process-id routes`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command is useful in isolating routing problems between the OSPF and the RTM. For example, if a route is missing from the RTM/FIB but is visible from the display output of this command, the problem is with downloading the route to the RTM.

This command has the following limitations:

- The display output is sorted by prefixes; intra-area ECMP routes are not displayed together.
- For Type 2 external routes, Type 1 cost is not displayed.

Example

```
FTOS#show ip ospf 100 route

Prefix        Cost Nexthop   Interface Area  Type
1.1.1.1        1   0.0.0.0   Lo 0      0     Intra-Area
3.3.3.3        2   13.0.0.3  Te 0/47   1     Intra-Area
13.0.0.0       1   0.0.0.0   Te 0/47   0     Intra-Area
150.150.150.0  2   13.0.0.3  Te 0/47   -     External
172.30.1.0     2   13.0.0.3  Te 0/47   1     Intra-Area
FTOS#
```

show ip ospf statistics

Display OSPF statistics.

S5000

Syntax

```
show ip ospf process-id statistics global | [interface name
{neighbor router-id}]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
global	Enter the keyword `global` to display the packet counts received on all running OSPF interfaces and packet counts received and transmitted by all OSPF neighbors.
interface *name*	(OPTIONAL) Enter the keyword `interface` followed by one of the following interface keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information. • For Port Channel groups, enter the keywords `port-channel` followed by a number. The range is 1 to 128. • For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.
neighbor *router-id*	(OPTIONAL) Enter the keyword `neighbor` followed by the neighbor's router-id in dotted decimal format (A.B.C.D.).

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output from the `show ip ospf statistics process-id global` command shown in the Example below.

Total	Displays the total number of packets received/transmitted by the OSPF process.
Error	Displays the error count while receiving and transmitting packets by the OSPF process.
Hello	Number of OSPF Hello packets.
DDiscr	Number of database description packets.

LSReq	Number of link state request packets.
LSUpd	Number of link state update packets.
LSAck	Number of link state acknowledgement packets.
TxQ-Len	The transmission queue length.
RxQ-Len	The reception queue length.
Tx-Mark	The highest number mark in the transmission queue.
Rx-Mark	The highest number mark in the reception queue.
Hello-Q	The queue, for transmission or reception, for the hello packets.
LSR-Q	The queue, for transmission or reception, for the link state request packets.
Other-Q	The queue, for transmission or reception, for the link state acknowledgement, database description, and update packets.

The following describes the error definitions for the `show ip ospf statistics` *`process-id`* `global` command.

Intf_Down	Received packets on an interface that is either down or OSPF is not enabled.
Non-Dr	Received packets with a destination address of ALL_DRS even though SELF is not a designated router.
Self-Org	Receive the self originated packet.
Wrong_Len	The received packet length is different to what was indicated in the OSPF header.
Invld-Nbr	LSA, LSR, LSU, and DDB are received from a peer which is not a neighbor peer.
Nbr-State	LSA, LSR, and LSU are received from a neighbor with stats less than the loading state.
Auth-Error	Simple authentication error.
MD5-Error	MD5 error
Cksum-Err	Checksum Error
Version	Version mismatch
AreaMismatch	Area mismatch
Conf-Issue	The received hello packet has a different hello or dead interval than the configuration.
No-Buffer	Buffer allocation failure.
Seq-no	A sequence no errors occurred during the database exchange process.
Socket	Socket Read/Write operation error.
Q-overflow	Packet(s) dropped due to queue overflow.

Unknown-Pkt	Received packet is not an OSPF packet.

Example

```
FTOS#show ip ospf 1 statistics global

OSPF Packet Count
   Total Error Hello DDiscr LSReq LSUpd LSAck
RX 10    0     8     2      0     0     0
TX 10    0     10    0      0     0     0

OSPF Global Queue Length
         TxQ-Len RxQ-Len Tx-Mark Rx-Mark
Hello-Q  0       0       0       2
LSR-Q    0       0       0       0
Other-Q  0       0       0       0

Error packets (Only for RX)

Intf-Down  0   Non-Dr     0   Self-Org 0
Wrong-Len  0   Invld-Nbr  0   Nbr-State 0
Auth-Err   0   MD5-Err    0   Chksum 0
Version    0   AreaMis    0   Conf-Issues 0
No-Buffer  0   Seq-No     0   Socket 0
Q-OverFlow 0   Unkown-Pkt 0

Error packets (Only for TX)

Socket Errors    0
FTOS#
```

Usage Information

The `show ip ospf` *`process-id`* `statistics` command displays the error packet count received on each interface as:

- The hello-timer remaining value for each interface
- The wait-timer remaining value for each interface
- The grace-timer remaining value for each interface
- The packet count received and transmitted for each neighbor
- Dead timer remaining value for each neighbor
- Transmit timer remaining value for each neighbor
- The LSU Q length and its highest mark for each neighbor
- The LSR Q length and its highest mark for each neighbor

Example (Statistics)

```
FTOS#show ip ospf 100 statistics

Interface TenGigabitEthernet 0/8

  Hello-Timer 9, Wait-Timer 0, Grace-Timer 0
  Error packets (Only for RX)

Intf-Down  0  Non-Dr       0  Self-Org    0
Wrong-Len  0  Invld-Nbr    0  Nbr-State   0
Auth-Error 0  MD5-Error    0  Cksum-Err   0
Version    0  AreaMisMatch 0  Conf-Issue  0
SeqNo-Err  0  Unkown-Pkt   0

  Neighbor ID 9.1.1.2

    Hello DDiscr LSReq LSUpd LSAck
RX  59    3      1     1     1
```

```
TX   62     2       1      0      0

  Dead-Timer  37, Transmit-Timer  0
  LSU-Q-Len    0, LSU-Q-Wmark     0
  LSR-Q-Len    0, LSR-Q-Wmark     1
```

Related Commands clear ip ospf statistics – clears the packet statistics in all interfaces and neighbors.

show ip ospf timers rate-limit

Show the LSA currently in the queue waiting for timers to expire.

S5000

Syntax `show ip ospf process-id timers rate-limit`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip ospf 10 timers rate-limit

List of LSAs in rate limit Queue
LSA id: 1.1.1.0 Type: 3 Adv Rtid: 3.3.3.3 Expiry time:
00:00:09.111
LSA id: 3.3.3.3 Type: 1 Adv Rtid: 3.3.3.3 Expiry time:
00:00:23.96
FTOS#
```

show ip ospf topology

Display routers in directly connected areas.

S5000

Syntax `show ip ospf process-id topology`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use this command to isolate problems with inter-area and external routes. In OSPF inter-area and external routes are calculated by adding LSA cost to the cost of reaching the router. If an inter-area or external route is not of correct cost, the display can determine if the path to the originating router is correct or not.

Example

```
FTOS#show ip ospf 1 topology

Router ID  Flags Cost  Nexthop   Interface Area
3.3.3.3    E/B/-/ 1    20.0.0.3  Te 13/1   0
1.1.1.1    E/-/-/ 1    10.0.0.1  Te 7/1    1
FTOS#
```

show ip ospf virtual-links

Display the OSPF virtual links configured and is useful for debugging OSPF routing operations. If no OSPF virtual-links are enabled on the switch, no output is generated.

S5000

Syntax

`show ip ospf process-id virtual-links`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output from the `show ip ospf process-id virtual-links` command shown in the Example below.

Virtual Link...	This line specifies the OSPF neighbor to which the virtual link was created and the link's status.

Run as...	This line states the nature of the virtual link.
Transit area...	This line identifies the area through which the virtual link was created, the interface used, and the cost assigned to that link.
Transmit Delay...	This line displays the transmit delay assigned to the link and the State of the OSPF neighbor.
Timer intervals...	This line displays the timer values assigned to the virtual link. The timers are Hello is hello-interval, Dead is dead-interval, Wait is transmit-delay, and Retransmit is retransmit-interval.
Hello due...	This line displays the amount of time until the next Hello packet is expected from the neighbor router.
Adjacency State...	This line displays the adjacency state between neighbors.

Example

```
FTOS#show ip ospf 1 virt

Virtual Link to router 192.168.253.5 is up
  Run as demand circuit
  Transit area 0.0.0.1, via interface TenGigabitEthernet
13/16, Cost of using 2
  Transmit Delay is 1 sec, State POINT_TO_POINT,
     Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
     Hello due in 00:00:02
FTOS#
```

summary-address

Set the OSPF ASBR to advertise one external route.

S5000

Syntax

`summary-address` *`ip-address mask`* `[not-advertise] [tag` *`tag-value`*`]`

To disable summary address, use the `no summary-address` *`ip-address mask`* command.

Parameters

ip-address	Specify the IP address in dotted decimal format of the address to be summarized.
mask	Specify the mask in dotted decimal format of the address to be summarized.
not-advertise	(OPTIONAL) Enter the keywords `not-advertise` to suppress that match the network prefix/mask pair.
tag *tag-value*	(OPTIONAL) Enter the keyword `tag` followed by a value to match on routes redistributed through a route map. The range is 0 to 4294967295.

Defaults Not configured.

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `area range` command summarizes routes for the different areas.

With the `not-advertise` parameter configured, you can use this command to filter out some external routes. For example, if you want to redistribute static routes to OSPF, but you don't want OSPF to advertise routes with prefix 1.1.0.0, you can configure the summary-address 1.1.0.0 255.255.0.0 not-advertise to filter out all the routes fall in range 1.1.0.0/16.

Related Commands

area range – summarizes routes within an area.

timers spf

Set the time interval between when the switch receives a topology change and starts a shortest path first (SPF) calculation.

S5000

Syntax

`timers spf` *`delay holdtime`*

To return to the default, use the `no timers spf` command.

Parameters

delay	Enter a number as the delay. The range is 0 to 4294967295. The default is **5 seconds**.
holdtime	Enter a number as the hold time. The range is 0 to 4294967295. The default is **10 seconds**.

Defaults

- delay = 5 seconds
- holdtime = 10 seconds

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Setting the *delay* and *holdtime* parameters to a low number enables the switch to switch to an alternate path quickly but requires more CPU usage.

timers throttle lsa all

Configure LSA transmit intervals.

S5000

Syntax

```
timers throttle lsa all {start-interval | hold-interval | max-
interval}
```

To return to the default, use the `no timers throttle lsa` command.

Parameters

start-interval	Set the minimum interval between initial sending and resending the same LSA. The range is 0 to 600,000 milliseconds.
hold-interval	Set the next interval to send the same LSA. This is the time between sending the same LSA after the start-interval has been attempted. The range is 1 to 600,000 milliseconds.
max-interval	Set the maximum amount of time the system waits before sending the LSA. The range is 1 to 600,000 milliseconds.

Defaults

- start-interval : **0 msec**
- hold-interval : **5000 msec**
- max-interval : **5000 msec**

Command Modes ROUTER OSPF

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

LSAs are sent after the start-interval and then after hold-interval until the maximum interval is reached. In throttling, exponential backoff is used when sending same LSA, so that the interval is multiplied until the maximum time is reached. For example, if the *start-interval 5000* and *hold-interval 1000* and *max-interval 100,000*, the LSA is sent at 5000 msec, then 1000 msec, then 2000 msec, them 4000 until 100,000 msec is reached.

timers throttle lsa arrival

Configure the LSA acceptance intervals.

S5000

Syntax

```
timers throttle lsa arrival arrival-time
```

To return to the default, use the `no timers throttle lsa` command.

Parameters

arrival-time	Set the interval between receiving the same LSA repeatedly, to allow sufficient time for the system to accept the LSA. The range is 0 to 600,000 milliseconds.

Defaults	1000 msec
Command Modes	ROUTER OSPF
Command History	

Version 9.0(1.3)	Introduced on the S5000.

38

Policy-based Routing (PBR)

Policy-based routing (PBR) allows you to apply routing policies to specific interfaces. To enable PBR, create a redirect list and apply it to the interface. After the redirect list is applied to the interface, all traffic passing through the interface is subject to the rules defined in the redirect list. FTOS supports PBR on the S5000 switch.

You can apply PBR to physical interfaces and logical interfaces (such as a link aggregation group [LAG] or virtual local area network [VLAN]). Trace lists and redirect lists do not function correctly when you configure both in the same configuration.

NOTE: Apply PBR to Layer 3 interfaces only.

description

Add a description to this redirect list.

S5000

Syntax `description {description}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description to identify the IP redirect list (80 characters maximum).

Defaults none

Command Modes REDIRECT-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands ip redirect-list – enables an IP Redirect List.

ip redirect-group

Apply a redirect list (policy-based routing) on an interface. You can apply multiple redirect lists to an interface by entering this command multiple times.

S5000

Syntax

`ip redirect-group` *`redirect-list-name`*

To remove a redirect list from an interface, use the `no ip redirect-group` *`name`* command.

Parameters

redirect-list-name	Enter the name of a configured redirect list.

Defaults

none

Command Modes

INTERFACE (conf-if-vl-)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can apply any number of redirect-groups to an interface. A redirect list can contain any number of configured rules. These rules includes the next-hop IP address where the incoming traffic is to be redirected.

If the next hop address is reachable, traffic is forwarded to the specified next hop. Otherwise the normal routing table is used to forward traffic. When a redirect-group is applied to an interface and the next-hop is reachable, the rules are added into the PBR CAM region. When incoming traffic hits an entry in the CAM, the traffic is redirected to the corresponding next-hop IP address specified in the rule.

NOTE: Apply the redirect list to physical, VLAN, or LAG interfaces only.

Related Commands

- show cam pbr – displays the content of the PBR CAM.
- show ip redirect-list – displays the redirect-list configuration.

ip redirect-list

Configure a redirect list and enter REDIRECT-LIST mode.

S5000

Syntax

`ip redirect-list` *`redirect-list-name`*

To remove a redirect list, use the `no ip redirect-list` command.

Parameters

redirect-list-name	Enter the name of a redirect list.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

permit

Configure a rule for the redirect list.

S5000

Syntax

```
permit {ip-protocol-number | protocol-type} {source mask | any
| host ip-address} {destination mask | any | host ip-address}
[bit] [operators]
```

To remove the rule, use one of the following:

- If you know the filter sequence number, use the `no seq sequence-number syntax` command.
- You can also use the `no permit {ip-protocol-number | protocol-type} {source mask | any | host ip-address} {destination mask | any | host ip-address} [bit] [operators]` command.

Parameters

ip-protocol-number	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
protocol-type	Enter one of the following keywords as the protocol type: • `icmp` for internet control message protocol • `ip` for any internet protocol • `tcp` for transmission control protocol • `udp` for user datagram protocol
source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all traffic is subject to the filter.
host *ip-address*	Enter the keyword `host` followed by the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.

bit	(OPTIONAL) For TCP protocol type only, enter one or a combination of the following TCP flags: • `ack` = acknowledgement • `fin` = finish (no more data from the user) • `psh` = push function • `rst` = reset the connection • `syn` = synchronize sequence number • `urg` = urgent field
operator	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • lt = less than • `range` = inclusive range of ports (you must specify two ports for the port command parameter.)

Defaults	none
Command Modes	REDIRECT-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

redirect

Configure a rule for the redirect list.

S5000

Syntax

```
redirect {ip-address} {ip-protocol-number | protocol-type
[bit]} {source mask | any | host ip-address} {destination mask
| any | host ip-address} [operator]
```

To remove this filter, use one of the following:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- You can also use the `no redirect {ip-address} {ip-protocol-number [bit] | protocol-type} {source mask | any | host ip-address} {destination mask | any | host ip-address} [operator]` command.

Parameters

ip-address	Enter the IP address of the forwarding router.

ip-protocol-number	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
protocol-type	Enter one of the following keywords as the protocol type: • `icmp` for internet control message protocol • `ip` for any internet protocol • `tcp` for transmission control protocol • `udp` for user datagram protocol
bit	(OPTIONAL) For TCP protocol type only, enter one or a combination of the following TCP flags: • `ack` = acknowledgement • `fin` = finish (no more data from the user) • `psh` = push function • `rst` = reset the connection • `syn` = synchronize sequence number • `urg` = urgent field
source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all traffic is subject to the filter.
host *ip-address*	Enter the keyword `host` followed by the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
operator	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the port command parameter.)

Defaults	none	
Command Modes	REDIRECT-LIST	
Command History	**Version 9.0(1.3)**	Introduced on the S5000.

seq

Configure a filter with an assigned sequence number for the redirect list.

S5000

Syntax

```
seq sequence-number {permit | redirect {ip-address} {ip-
protocol-number | protocol-type} {source mask | any | host ip-
address} {destination mask | any | host ip-address} [bit]
[operator]
```

To delete a filter, use the `no seq sequence-number` command.

Parameters

sequence-number	Enter a number from 1 to 65535.
permit	Enter the keyword `permit` assign the sequence to the permit list.
redirect	Enter the keyword `redirect` to assign the sequence to the redirect list.
ip-address	Enter the IP address of the forwarding router.
ip-protocol-number	ip-protocol-number Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
protocol-type	Enter one of the following keywords as the protocol type: • `icmp` for internet control message protocol • `ip` for any internet protocol • `tcp` for transmission control protocol • `udp` for user datagram protocol
source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all traffic is subject to the filter.
host *ip-address*	Enter the keyword `host` followed by the IP address to specify a host IP address.
destination	destination Enter the IP address of the network or host to which the packets are sent.
bit	(OPTIONAL) For TCP protocol type only, enter one or a combination of the following TCP flags: • `ack` = acknowledgement • `fin` = finish (no more data from the user) • `psh` = push function • `rst` = reset the connection • `syn` = synchronize sequence number • `urg` = urgent field

operator	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt`= less than • `range` = inclusive range of ports (you must specify two ports for the port command parameter.)

Defaults none

Command Modes REDIRECT-LIST

Command History

Version 9.0(1.3)	Introduced on the S5000.

show ip redirect-list

View the redirect list configuration and the interfaces it is applied to.

S5000

Syntax `show ip redirect-list` *`redirect-list-name`*

Parameters

redirect-list-name	Enter the name of a configured Redirect list.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The `show cam pbr` command displays the PBR CAM content. The “VlanID” column displays the corresponding VLAN ID to which the redirect-group is applied.

Example

```
FTOS#show ip redirect-list test

IP redirect-list rcl0:
 Defined as:
  seq 5 permit ip any host 182.16.2.10
  seq 10 redirect 182.16.1.2 ip any any, Next-hop un-
reachable, ARP un-resolved
 Applied interfaces:
  Te 9/0
  So 8/2
  Vl 10
  Po 3
FTOS#
```

39

PIM-Sparse Mode (PIM-SM)

FTOS supports protocol-independent multicast (PIM) commands on the S5000 switch.

This chapter contains the following sections:

- IPv4 PIM-Sparse Mode Commands
- IPv6 PIM-Sparse Mode Commands

IPv4 PIM-Sparse Mode Commands

The following describes the IPv4 PIM-sparse mode (PIM-SM) commands.

clear ip pim rp-mapping

Used by the bootstrap router (BSR) to remove all or particular rendezvous point (RP) advertisement.

S5000

Syntax `clear ip pim rp-mapping rp-address`

Parameters

rp-address	(OPTIONAL) Enter the RP address in dotted decimal format (A.B.C.D).

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ip pim tib

Clear PIM tree information from the PIM database.

S5000

Syntax `clear ip pim tib [group]`

Parameters	**group**	(OPTIONAL) Enter the multicast group address in dotted decimal format (A.B.C.D).
Command Modes	EXEC Privilege	
Command History	**Version 9.0(1.3)**	Introduced on the S5000.

clear ip pim snooping tib

Clear tree information discovered by PIM-SM snooping from the PIM database.

S5000

Syntax

```
clear ip pim snooping tib [vlan vlan-id] [group-address]
```

Parameters	**vlan** ***vlan-id***	(OPTIONAL) Enter a VLAN ID to clear tree information base (TIB) information learned through PIM-SM snooping about a specified VLAN. The valid VLAN IDs are 1 to 4094.
	group-address	(OPTIONAL) Enter a multicast group address in dotted decimal format (A.B.C.D) to clear TIB information learned through PIM-SM snooping about a specified multicast group.
Command Modes	EXEC Privilege	
Command History	**Version 9.0(1.3)**	Introduced on the S5000.
Related Commands	show ip pim snooping tib – displays TIB information learned through PIM-SM snooping.	

debug ip pim

View IP PIM debugging messages.

S5000

Syntax

```
debug ip pim [bsr | events | group | packet [in | out] |
register | state | timer [assert | hello | joinprune |
register]]
```

To disable PIM debugging, use the `no debug ip pim` command or use the `undebug all to disable all debugging` command.

Parameters

bsr	(OPTIONAL) Enter the keyword `bsr` to view PIM Candidate RP/BSR activities.
events	(OPTIONAL) Enter the keyword `group` to view PIM messages for a specific group.
group	(OPTIONAL) Enter the keyword `group` to view PIM messages for a specific group.
packet [in | out]	(OPTIONAL) Enter the keyword `packet` to view PIM packets. Enter one of the optional parameters: • `in`: to view incoming packets • `out`: to view outgoing packets
register	(OPTIONAL) Enter the keyword `register` to view PIM register address in dotted decimal format (A.B.C.D).
state	(OPTIONAL) Enter the keyword `state` to view PIM state changes.
timer [assert | hello | joinprune | register]	(OPTIONAL) Enter the keyword `timer` to view PIM timers. Enter one of the optional parameters: • `assert`: to view the assertion timer • `hello`: to view the PIM neighbor keepalive timer • `joinprune`: to view the expiry timer (join/prune timer) • `register`: to view the register suppression timer

Defaults Disabled.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip pim bsr-border

Define the border of PIM domain by filtering inbound and outbound PIM-BSR messages per interface.

S5000

Syntax `ip pim bsr-border`

To return to the default value, use the `no ip pim bsr-border` command.

Defaults Disabled.

Command Modes INTERFACE

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Usage Information

This command is applied to the subsequent PIM-BSR. Existing BSR advertisements are cleaned up by time out. Candidate RP advertisements can be cleaned using the `clear ip pim rp-mapping` command.

ip pim bsr-candidate

Configure the PIM router to join the Bootstrap election process.

S50000

Syntax

`ip pim bsr-candidate` *`interface-type slot/port`* `[`*`hash-mask-length`*`] [`*`priority`*`]`

To return to the default value, use the `no ip pim bsr-candidate` command.

Parameters

interface-type slot/port	Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
hash-mask-length	(OPTIONAL) Enter the hash mask length. The range is zero (0) to 32. The default is **30**.
priority	(OPTIONAL) Enter the priority used in Bootstrap election process. The range is zero (0) to 255. The default is **zero (0)**.

Defaults Not configured.

Command Modes CONFIGURATION

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

ip pim dr-priority

Change the designated router (DR) priority for the interface.

S5000

Syntax

```
ip pim dr-priority priority-value
```

To remove the DR priority value assigned, use the `no ip pim dr-priority` command.

Parameters

priority-value	Enter a number. Preference is given to larger/higher number. The range is 0 to 4294967294. The default is 1.

Defaults 1

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The router with the largest value assigned to an interface becomes the designated router. If two interfaces contain the same designated router priority value, the interface with the largest interface IP address becomes the designated router.

ip pim graceful-restart

This feature permits configuration of non-stop forwarding (NSF or graceful restart) capability of a PIM router to its neighbors.

S5000

Syntax

```
[ipv6] ip pim graceful-restart {helper-only | nsf [restart-time
| stale-entry-time]}
```

Parameters

ipv6	Enter the keyword `ipv6` to enable graceful-restart for the IPv6 multicast routes.
helper-only	Enter the keywords `helper-only` to configure as a receiver (helper) only by preserving the PIM status of a graceful restart PIM neighboring router.
nsf	Enter the keyword `nsf` to configure the non-stop forwarding capability.
restart-time	(OPTIONAL) Enter the keywords `restart-time` followed by the number of seconds estimated for the PIM speaker to restart. The range is 30 to 300 seconds. The default is **180 seconds**.
stale-entry-time	(OPTIONAL) Enter the keywords `stale-entry-time` followed by the number of seconds for which entries are kept alive after restart. The range is 30 to 300 seconds. The default is **60 seconds**.

Defaults	as above
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	When an NSF-capable router comes up, it announces the graceful restart capability and restart duration as a `Hello` option. The receiving router notes the `Hello` option. Routers not NSF-capable discard the unknown `Hello` option and adjacency is not affected. When an NSF-capable router goes down, the neighboring PIM speaker preserves the states and continues the forwarding of multicast traffic while the neighbor router restarts.

ip pim join-filter

Permit or deny PIM Join/Prune messages on an interface using an extended IP access list. This command prevents the PIM-SM router from creating state based on multicast source and/or group.

S5000

Syntax

`ip pim join-filter ext-access-list {in | out}`

To remove the access list, use the `no ip pim join-filter ext-access-list {in | out}` command.

Parameters

ext-access-list	Enter the name of an extended access list.
in	Enter this keyword to apply the access list to inbound traffic.
out	Enter this keyword to apply the access list to outbound traffic.

Defaults	none
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
FTOS(conf)# ip access-list extended iptv-channels
FTOS(config-ext-nacl)# permit ip 10.1.2.3/24 225.1.1.0/24
FTOS(config-ext-nacl)# permit ip any 232.1.1.0/24
FTOS(config-ext-nacl)# permit ip 100.1.1.0/16 any
FTOS(config-if-te-1/1)# ip pim join-filter iptv-channels in
FTOS(config-if-te-1/1)# ip pim join-filter iptv-channels out
```

Related Commands

ip access-list extended – configure an access list based on IP addresses or protocols.

ip pim ingress-interface-map

When the Dell Networking system is the RP, statically map potential incoming interfaces to (*,G) entries to create a lossless multicast forwarding environment.

S5000

Syntax

`ip pim ingress-interface-map` *`std-access-list`*

Parameters

std-access-list	Enter the name of an standard access list.

Defaults

none

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf)# ip access-list standard map1
FTOS(config-std-nacl)# permit 224.0.0.1/24
FTOS(config-std-nacl)#exit
FTOS(conf)#int tengig 1/1
FTOS(config-if-te-1/1)# ip pim ingress-interface-map map1
```

ip pim neighbor-filter

Configure this feature to prevent a router from participating in protocol independent multicast (PIM).

S5000

Syntax

`ip pim neighbor-filter {`*`access-list`*`}`

To remove the restriction, use the `no ip pim neighbor-filter {access-list}` command.

Parameters

access-list	Enter the name of a standard access list. Maximum 16 characters.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Do not enter this command before creating the access-list.

ip pim query-interval

Change the frequency of PIM Router-Query messages.

S5000

Syntax	`ip pim query-interval seconds` To return to the default value, use the `no ip pim query-interval seconds` command.
Parameters	*seconds* — Enter a number as the number of seconds between router query messages. The range: 0 to 65535. The default is **30 seconds**.
Defaults	**30 seconds**
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

ip pim register-filter

Use this feature to prevent a PIM source DR from sending register packets to an RP for the specified multicast source and group.

S5000

Syntax	`ip pim register-filter access-list` To return to the default, use the `no ip pim register-filter access-list` command.
Parameters	*access-list* — Enter the name of an extended access list. Maximum 16 characters.
Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** — Introduced on the S5000.
Usage Information	The access name is an extended IP access list that denies PIM register packets to RP at the source DR based on the multicast and group addresses. Do not enter this command before creating the access-list.

ip pim rp-address

Configure a static PIM rendezvous point (RP) address for a group or access-list.

S5000

Syntax	`ip pim rp-address` *`address`* `{group-address` *`group-address mask`*`} override` To remove an RP address, use the `no ip pim rp-address` *`address`* `{group-address` *`group-address mask`*`} override` command.
Parameters	

address	Enter the RP address in dotted decimal format (A.B.C.D).
group-address *group-address mask*	Enter the keywords `group-address` followed by a group-address mask, in dotted decimal format (/xx), to assign that group address to the RP.
override	Enter the keyword `override` to override the BSR updates with static RP. The override takes effect immediately during enable/ disable. **NOTE:** This option is applicable to multicast group range.

Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	This address is used by first-hop routers to send register packets on behalf of source multicast hosts. The RP addresses are stored in the order in which they are entered. RP addresses learned using BSR take priority over static RP addresses. Without the `override` option, RPs advertised by the BSR updates take precedence over the statically configured RPs.

ip pim rp-candidate

Configure a PIM router to send out a Candidate-RP-Advertisement message to the bootstrap (BS) router or define group prefixes that are defined with the RP address to PIM BSR.

S5000

Syntax	`ip pim rp-candidate {`*`interface`* `[`*`priority`*`]` To return to the default value, use the `no ip pim rp-candidate {`*`interface`* `[`*`priority`*`]` command.
Parameters	

interface	Enter the following keywords and slot/port or number information:

- For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number. The range is 1 to 128.
- For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

priority	(OPTIONAL) Enter the priority used in Bootstrap election process. The range is zero (0) to 255. The default is **192**.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Priority is stored at BSR router when receiving a Candidate-RP-Advertisement.

ip pim snooping

Enable PIM-SM snooping globally on a switch or on a VLAN interface.

S5000

Syntax `ip pim snooping [enable]`

To disable PIM-SM snooping, use the `no ip pim snooping [enable]` command.

Defaults Disabled.

Command Modes

- CONFIGURATION: To configure PIM-SM snooping globally, enter the `ip pim snooping enable` command in global configuration mode.
- VLAN INTERFACE: To configure PIM-SM snooping on a VLAN interface, enter the `ip pim snooping` command in VLAN interface configuration mode.

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Because PIM-SM snooping is used in a Layer 2 environment, PIM-SM snooping and PIM multicast routing are mutually exclusive. PIM-SM snooping cannot be enabled on a switch/router if PIM-SM or PIM-DM is enabled.

If enabled at the global level, PIM-SM snooping is automatically enabled on all VLANs unless the `no ip pim snooping` command has been entered on a VLAN.

If enabled at the VLAN level, PIM-SM snooping requires that you also enter the `no shutdown` command to enable the interface.

PIM-SM snooping is supported with IGMP snooping, and forwards the IGMP report on the port that connects to the PIM DR. Dell Networking recommends that you do not enable IGMP snooping on a PIM-SM snooping-enabled VLAN interface unless until it is necessary for VLAN operation.

PIM-SM snooping listens to PIM hello and PIM-SM join and prune messages while maintaining the VLAN- and port-specific information in multicast packets that are snooped.

To display information about the operation of PIM-SM snooping on a switch, enter the `show ip pim summary` command.

Related Commands

show ip pim snooping tib – displays TIB information learned through PIM-SM snooping.

ip pim sparse-mode

Enable PIM sparse mode and IGMP on the interface.

S5000

Syntax

`ip pim sparse-mode`

To disable PIM sparse mode and IGMP, use the `no ip pim sparse-mode` command.

Defaults

Disabled.

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The interface must be enabled (the `no shutdown` command) and not have the `switchport` command configured. Multicast must also be enabled globally (using the `ip multicast-lag-hashing` command). PIM is supported on the port-channel interface.

Related Commands

ip multicast-lag-hashing – enables multicast globally.

ip pim sparse-mode sg-expiry-timer

Enable expiry timers globally for all sources, or for a specific set of (S,G) pairs defined by an access list.

S5000

Syntax

`ip pim sparse-mode sg-expiry-timer *seconds* [access-list name]`

To disable configured timers and return to default mode, use the `no ip pim sparse-mode sg-expiry-timer` command.

Parameters

seconds	Enter the number of seconds the S, G entries are retained. The range is 211 to 86400.
access-list name	(OPTIONAL) Enter the name of a previously configured Extended ACL to enable the expiry time to specified S,G entries.

Defaults

Disabled. The default expiry timer (with no times configured) is 210 sec.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command configures an expiration timer for all S.G entries, unless they are assigned to an Extended ACL.

ip pim spt-threshold

Configure the PIM router to switch to the shortest path tree when the traffic reaches the specified threshold value.

S5000

Syntax

`ip pim spt-threshold *value* | infinity`

To return to the default value, use the `no ip pim spt-threshold` command.

Parameters

value	(OPTIONAL) Enter the traffic value in kilobits per second. The default is **10 packets per second**. A value of zero (0) causes a switchover on the first packet.
infinity	(OPTIONAL) Enter the keyword `infinity` to never switch to the source-tree.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	This is applicable to last hop routers on the shared tree towards the rendezvous point (RP).

no ip pim snooping dr-flood

Disable the flooding of multicast packets to the PIM designated router.

S5000

Syntax

```
no ip pim snooping dr-flood
```

To re-enable the flooding of multicast packets to the PIM designated router, use the `ip pim snooping dr-flood` command.

Defaults

Enabled.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

By default, when you enable PIM-SM snooping, a switch floods all multicast traffic to the PIM designated router (DR), including unnecessary multicast packets. To minimize the traffic sent over the network to the designated router, you can disable `designated-router flooding`.

When designated-router flooding is disabled, PIM-SM snooping only forwards the multicast traffic, which belongs to a multicast group for which the switch receives a join request, on the port connected towards the designated router.

If the PIM DR flood is not disabled (default setting):

- Multicast traffic is transmitted on the egress port towards the PIM DR if the port is not the incoming interface.
- Multicast traffic for an unknown group is sent on the port towards the PIM DR. When DR flooding is disabled, multicast traffic for an unknown group is dropped.

Related Commands

ip pim snooping – enables PIM-SM snooping.

show ip pim bsr-router

View information on the Bootstrap router.

S5000

Syntax

```
show ip pim bsr-router
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
  BSR address: 7.7.7.7 (?)
  Uptime: 16:59:06, BSR Priority: 0, Hash mask length: 30
  Next bootstrap message in 00:00:08

This system is a candidate BSR
  Candidate BSR address: 7.7.7.7, priority: 0, hash mask
length: 30
FTOS#
```

show ip pim interface

View information on the interfaces with IP PIM enabled.

S5000

Syntax `show ip pim interface`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip pim interface` command shown in the Example below.

Field	Description
Address	Lists the IP addresses of the interfaces participating in PIM.
Interface	List the interface type, with either slot/port information or ID (VLAN or Port Channel), of the interfaces participating in PIM.
Ver/Mode	Displays the PIM version number and mode for each interface participating in PIM: • v2 = PIM version 2 • S = PIM Sparse mode

Field	Description
Nbr Count	Displays the number of PIM neighbors discovered over this interface.
Query Intvl	Displays the query interval for Router Query messages on that interface (configured with `ip pim query-interval` command).
DR Prio	Displays the Designated Router priority value configured on the interface (use the `ip pim dr-priority` command).
DR	Displays the IP address of the Designated Router for that interface.

Example

```
FTOS#show ip pim interface
Address        Interface Ver/ Nbr   Query DR   DR
                         Mode Count Intvl Prio
172.21.200.254 Te 7/9    v2/S 0     30 1  172.21.200.254
172.60.1.2     Te 7/11   v2/S 0     30 1  172.60.1.2
192.3.1.1      Te 7/16   v2/S 1     30 1  192.3.1.1
192.4.1.1      Te 13/5   v2/S 0     30 1  192.4.1.1
172.21.110.1   Te 13/6   v2/S 0     30 1  172.21.110.1
172.21.203.1   Te 13/7   v2/S 0     30 1  172.21.203.1
FTOS#
```

show ip pim neighbor

View PIM neighbors.

S5000

Syntax

```
show ip pim neighbor
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output from the `show ip pim neighbor` command shown in the Example below.

Field	Description
Neighbor address	Displays the IP address of the PIM neighbor.
Interface	List the interface type, with either slot/port information or ID (VLAN or Port Channel), on which the PIM neighbor was found.
Uptime/expires	Displays the amount of time the neighbor has been up followed by the amount of time until the neighbor is removed from the multicast routing table (that is, until the neighbor hold time expires).

Ver	Displays the PIM version number. - v2 = PIM version 2
DR prio/Mode	Displays the Designated Router priority and the mode. - 1 = default Designated Router priority (use the `ip pim dr-priority` command) - DR = Designated Router - S = Sparse mode

Example

```
FTOS#show ip pim neighbor
Neighbor   Interface  Uptime/Expires    Ver   DR
Address                                       Prio/Mode
127.87.3.4 Te 7/16    09:44:58/00:01:24  v2   1 / S
FTOS#
```

show ip pim rp

View all multicast groups-to-RP mappings.

S5000

Syntax `show ip pim rp [mapping | group-address]`

Parameters

mapping	(OPTIONAL) Enter the keyword `mapping` to display the multicast groups-to-RP mapping and information on how RP is learnt.
group-address	(OPTIONAL) Enter the multicast group address mask in dotted decimal format to view RP for a specific group.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#sh ip pim rp
Group            RP
224.2.197.115    165.87.20.4
224.2.217.146    165.87.20.4
224.3.3.3        165.87.20.4
225.1.2.1        165.87.20.4
225.1.2.2        165.87.20.4
229.1.2.1        165.87.20.4
229.1.2.2        165.87.20.4
FTOS#
```

Example (Mapping)

```
FTOS#sh ip pim rp mapping
Group(s): 224.0.0.0/4
  RP: 165.87.20.4, v2
    Info source: 165.87.20.5, via bootstrap, priority 0
      Uptime: 00:03:11, expires: 00:02:46
  RP: 165.87.20.3, v2
    Info source: 165.87.20.5, via bootstrap, priority 0
      Uptime: 00:03:11, expires: 00:03:03

FTOS#
```

Example (Address)

```
FTOS#sh ip pim rp 229.1.2.1
Group          RP
229.1.2.1    165.87.20.4

FTOS#
```

show ip pim snooping interface

Display information on VLAN interfaces with PIM-SM snooping enabled.

S5000

Syntax `show ip pim snooping interface [vlan vlan-id]`

Parameters

vlan *vlan-id*	(OPTIONAL) Enter a VLAN ID to display information about a specified VLAN configured for PIM-SM snooping. The valid VLAN IDs range is 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip pim snooping interface` commands shown in the Example below.

Field	Description
Interface	Displays the VLAN interfaces with PIM-SM snooping enabled.
Ver/Mode	Displays the PIM version number for each VLAN interface with PIM-SM snooping enabled: • v2 = PIM version 2 • S = PIM Sparse mode
Nbr Count	Displays the number of neighbors learned through PIM-SM snooping on the interface.

DR Prio	Displays the Designated Router priority value configured on the interface (`ip pim dr-priority` command).
DR	Displays the IP address of the Designated Router for that interface.

Example (#2)

```
FTOS#show ip pim snooping interface
Interface Ver Nbr    DR    DR
              Count  Prio
Vlan 2    v2  3      1     165.87.32.2
```

show ip pim snooping neighbor

Display information on PIM neighbors learned through PIM-SM snooping.

S5000

Syntax `show ip pim snooping neighbor [vlan vlan-id]`

Parameters

vlan *vlan-id*	(OPTIONAL) Enter a VLAN ID to display information about PIM neighbors that was discovered by PIM-SM snooping on a specified VLAN. The valid VLAN IDs range is 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output from the `show ip pim snooping neighbor` command shown in the Example below.

Field	**Description**
Neighbor address	Displays the IP address of the neighbor learned through PIM-SM snooping.
Interface	Displays the VLAN ID number and slot/port on which the PIM-SM-enabled neighbor was discovered.
Uptime/expires	Displays the amount of time the neighbor has been up followed by the amount of time until the neighbor is removed from the multicast routing table (that is, until the neighbor hold time expires).
Ver	Displays the PIM version number: • v2 = PIM version 2
DR prio/Mode	Displays the Designated Router priority and the mode:

- 1 = default Designated Router priority (use the `ip pim dr-priority` command)
- DR = Designated Router
- S = Sparse mode

Example

```
FTOS#show ip pim snooping neighbor

Neighbor    Interface          Uptime/Expires    Ver  DR Prio
Address
165.87.32.2   Vl 2 [Te 4/13 ]  00:04:03/00:01:42  v2  1
165.87.32.10  Vl 2 [Te 4/11 ]  00:00:46/00:01:29  v2  0
165.87.32.12  Vl 2 [Te 4/20 ]  00:00:51/00:01:24  v2  0
```

show ip pim snooping tib

Display information from the tree information base (TIB) discovered by PIM-SM snooping about multicast group members and states.

S5000

Syntax

`show ip pim snooping tib [vlan` *`vlan-id`*`] [`*`group-address`*` [`*`source-address`*`]]`

Parameters

vlan *vlan-id*	(OPTIONAL) Enter a VLAN ID to display TIB information discovered by PIM-SM snooping on a specified VLAN. The valid VLAN IDs range is 1 to 4094.
group-address	(OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D) to display TIB information discovered by PIM-SM snooping for a specified multicast group.
source-address	(OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D) to display TIB information discovered by PIM-SM snooping for a specified multicast source.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output from the `show ip pim snooping tib` commands shown in the Example below.

Field	Description
(S, G)	Displays the entry in the PIM multicast snooping database.

uptime	Displays the amount of time the entry has been in the PIM multicast route table.
expires	Displays the amount of time until the entry expires and is removed from the database.
RP	Displays the IP address of the RP/source for this entry.
flags	List the flags to define the entries: • S = PIM Sparse Mode • C = directly connected • L = local to the multicast group • P = route was pruned • R = the forwarding entry is pointing toward the RP • F = FTOS is registering this entry for a multicast source • T = packets were received via Shortest Tree Path • J = first packet from the last hop router is received and the entry is ready to switch to SPT • K=acknowledge pending state
Incoming interface	Displays the reverse path forwarding (RPF) interface towards the RP/source.
RPF neighbor	Displays the next hop from this interface towards the RP/source.
Outgoing interface list:	Lists the interfaces that meet one of the following criteria: • a directly connect member of the Group • statically configured member of the Group • received a (*,G) Join message

Example

```
FTOS#show ip pim snooping tib

PIM Multicast Snooping Table
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
       SGR-P - (S,G,R) Prune
Timers: Uptime/Expires
* : Inherited port

(*, 225.1.2.1), uptime 00:00:01, expires 00:02:59, RP
165.87.70.1, flags: J
  Incoming interface: Vlan 2, RPF neighbor 0.0.0.0
  Outgoing interface list:
    TenGigabitEthernet 4/11 RPF 165.87.32.2 00:00:01/00:02:59
    TenGigabitEthernet 4/13 Upstream Port   -/-

FTOS#show ip pim snooping tib vlan 2 225.1.2.1 165.87.1.7

PIM Multicast Snooping Table
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
       SGR-P - (S,G,R) Prune
Timers: Uptime/Expires
* : Inherited port

(165.87.1.7, 225.1.2.1), uptime 00:00:08, expires 00:02:52,
flags: j
  Incoming interface: Vlan 2, RPF neighbor 0.0.0.0
  Outgoing interface list:
    TenGigabitEthernet 4/11 Upstream Port    -/-
    TenGigabitEthernet 4/13 DR Port          -/-
    TenGigabitEthernet 4/20 RPF 165.87.32.10 00:00:08/00:02:52
```

show ip pim summary

View information about PIM-SM operation.

S5000

Syntax `show ip pim summary`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ip pim summary

PIM TIB version 495
Uptime 22:44:52
Entries in PIM-TIB/MFC : 2/2

Active Modes :
        PIM-SNOOPING

Interface summary:
        1 active PIM interface
        0 passive PIM interfaces
        3 active PIM neighbors

TIB summary:
       1/1 (*,G) entries in PIM-TIB/MFC
       1/1 (S,G) entries in PIM-TIB/MFC
       0/0 (S,G,Rpt) entries in PIM-TIB/MFC

       0 PIM nexthops
       0 RPs
       0 sources
       0 Register states

Message summary:
       2582/2583 Joins sent/received
       5/0 Prunes sent/received
       0/0 Candidate-RP advertisements sent/received
       0/0 BSR messages sent/received
       0/0 State-Refresh messages sent/received
       0/0 MSDP updates sent/received
       0/0 Null Register messages sent/received
       0/0 Register-stop messages sent/received
```

```
Data path event summary:
       0 no-cache messages received
       0 last-hop switchover messages received
       0/0 pim-assert messages sent/received
       0/0 register messages sent/received

Memory usage:
       TIB              : 3768 bytes
       Nexthop cache    : 0 bytes
       Interface table : 992 bytes
       Neighbor table  : 528 bytes
       RP Mapping       : 0 bytes
```

show ip pim tib

View the PIM tree information base (TIB).

S5000

Syntax `show ip pim tib [group-address [source-address]]`

Parameters

group-address	(OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D).
source-address	(OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D).

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ip pim tib` command shown in the Example below.

Field	Description
(S, G)	Displays the entry in the multicast PIM database.
uptime	Displays the amount of time the entry has been in the PIM route table.
expires	Displays the amount of time until the entry expires and is removed from the database.
RP	Displays the IP address of the RP/source for this entry.
flags	List the flags to define the entries: • D = PIM Dense Mode • S = PIM Sparse Mode • C = directly connected

- L = local to the multicast group
- P = route was pruned
- R = the forwarding entry is pointing toward the RP
- F = FTOS is registering this entry for a multicast source
- T = packets were received via Shortest Tree Path
- J = first packet from the last hop router is received and the entry is ready to switch to SPT
- K = acknowledge pending state

Incoming interface	Displays the reverse path forwarding (RPF) interface towards the RP/ source.
RPF neighbor	Displays the next hop from this interface towards the RP/source.
Outgoing interface list:	Lists the interfaces that meet one of the following criteria: • a directly connect member of the Group • statically configured member of the Group • received a (*,G) Join message

Example

```
FTOS#show ip pim tib

PIM Multicast Routing Table
Flags:D- Dense, S- Sparse, C- Connected, L- Local, P- Pruned,
      R- RP-bit set, F- Register flag, T- SPT-bit set, J- Join
SPT,
      M- MSDP created entry, A- Candidate for MSDP
Advertisement,
      K- Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 226.1.1.1), uptime 01:29:19, expires 00:00:52, RP
10.211.2.1, flags: SCJ
  Incoming interface: TenGigabitEthernet 4/23, RPF neighbor
10.211.1.2
  Outgoing interface list:
    TenGigabitEthernet 8/0

(*, 226.1.1.2), uptime 00:18:08, expires 00:00:52, RP
10.211.2.1, flags: SCJ
  Incoming interface: TenGigabitEthernet 4/23, RPF neighbor
10.211.1.2
  Outgoing interface list:
    TenGigabitEthernet 8/0

(*, 226.1.1.3), uptime 00:18:08, expires 00:00:52, RP
10.211.2.1, flags: SCJ
  Incoming interface: TenGigabitEthernet 4/23, RPF neighbor
10.211.1.2
  Outgoing interface list:
    TenGigabitEthernet 8/0

(*, 226.1.1.4), uptime 00:18:08, expires 00:00:52, RP
10.211.2.1, flags: SCJ
  Incoming interface: TenGigabitEthernet 4/23, RPF neighbor
10.211.1.2
```

```
    Outgoing interface list:
      TenGigabitEthernet 8/0
```

show running-config pim

Display the current configuration of PIM-SM snooping.

S5000

Syntax `show running-config pim`

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show running-config pim
!
ip pim snooping enable
```

Related Commands ip pim snooping – enables PIM-SM snooping.

IPv6 PIM-Sparse Mode Commands

The following describes the IPv6 PIM-sparse mode (PIM-SM) commands.

clear ipv6 pim tib

Clear the IPv6 PIM multicast-routing database (tree information base—TIB).

S5000

Syntax `clear ipv6 pim tib [group-address]`

Parameters

group-address	(OPTIONAL) Enter the multicast group address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zero.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

show ipv6 pim tib – displays the IPv6 PIM tree information base (TIB)

debug ipv6 pim

Invoke IPv6 PIM debugging.

S5000

Syntax

```
debug ipv6 pim [bsr | events | group group | packet | register
[group] | state | | timer [assert | hello | joinprune |
register]]
```

To disable IPv6 PIM debugging, use the `no debug ipv6 pim` command.

Parameters

bsr	(OPTIONAL) Enter the keyword `bsr` to invoke debugging of IPv6 PIM Candidate RP/BSR activities.
events	(OPTIONAL) Enter the keyword `events` to invoke debugging of IPv6 PIM events.
group *group*	(OPTIONAL) Enter the keyword `group` followed by the group address to invoke debugging on that specific group.
packet	(OPTIONAL) Enter the keyword `packet` to invoke debugging of IPv6 PIM packets.
register [*group*]	(OPTIONAL) Enter the keyword `register` and optionally the group address to invoke debugging of IPv6 PIM register messages for a particular group.
state	(OPTIONAL) Enter the keyword `state` to view IPv6 PIM state changes.
timer [assert | hello | joinprune | register]	(OPTIONAL) Enter the keyword `timer` to view IPv6 PIM timers. Enter one of the optional parameters: • `assert`: to view the assertion timer • `hello`: to view the IPv6 PIM neighbor keepalive timer • `joinprune`: to view the expiry timer (join/prune timer) • `register`: to view the register suppression timer

Defaults Disabled.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

ipv6 pim bsr-border

Invoke IPv6 PIM debugging.

S5000

Syntax

```
debug ipv6 pim [bsr | events | group group | packet | register
[group] | state | | timer [assert | hello | joinprune |
register]]
```

To disable IPv6 PIM debugging, use the `no debug ipv6 pim` command.

Parameters

bsr	(OPTIONAL) Enter the keyword `bsr` to invoke debugging of IPv6 PIM Candidate RP/BSR activities.
events	(OPTIONAL) Enter the keyword `events` to invoke debugging of IPv6 PIM events.
group *group*	(OPTIONAL) Enter the keyword `group` followed by the group address to invoke debugging on that specific group.
packet	(OPTIONAL) Enter the keyword `packet` to invoke debugging of IPv6 PIM packets.
register [*group*]	(OPTIONAL) Enter the keyword `register` and optionally the group address to invoke debugging of IPv6 PIM register messages for a particular group.
state	(OPTIONAL) Enter the keyword `state` to view IPv6 PIM state changes.
timer [assert | hello | joinprune | register]	(OPTIONAL) Enter the keyword `timer` to view IPv6 PIM timers. Enter one of the optional parameters: • `assert`: to view the assertion timer • `hello`: to view the IPv6 PIM neighbor keepalive timer • `joinprune`: to view the expiry timer (join/prune timer) • `register`: to view the register suppression timer

Defaults Disabled.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

ipv6 pim bsr-candidate

Configure the router as a bootstrap (BSR) candidate.

S5000

Syntax

`ipv6 pim bsr-candidate` *`interface-type slot/port`* `[`*`hash-mask-length`*`] [`*`priority`*`]`

To disable the bootstrap candidate, use the `no ipv6 pim bsr-candidate` command.

Parameters

interface-type slot/port	Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
hash-mask-length	(OPTIONAL) Enter the hash mask length for RP selection. The range is 0 to 128. The default is **126**.
priority	(OPTIONAL) Enter the priority value for Bootstrap election process. The range is 0 to 255. The default is **0**.

Defaults Refer to Parameters.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

ipv6 pim dr-priority

Change the designated router (DR) priority for the IPv6 interface.

S5000

Syntax

`ipv6 pim dr-priority` *`priority-value`*

To remove the DR priority value assigned, use the `no ipv6 pim dr-priority` command.

Parameters

priority-value	Enter a number. Preference is given to larger/higher number. The range is 0 to 4294967294. The default is **1**.

Defaults 1

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The router with the largest value assigned to an interface becomes the designated router. If two interfaces contain the same designated router priority value, the interface with the largest interface IP address becomes the designated router.

ipv6 pim join-filter

Permit or deny PIM Join/Prune messages on an interface using an access list. This command prevents the PIM-SM router from creating state based on multicast source and/or group.

S5000

Syntax `ipv6 pim join-filter access-list`

Parameters

access-list	Enter the name of an extended access list.
in	Enter the keyword `in` to apply the access list to inbound traffic.
out	Enter the keyword `out` to apply the access list to outbound traffic.

Defaults none

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf)#ipv6 access-list JOIN-FIL_ACL
FTOS(conf-ipv6-acl)#permit ipv6 165:87:34::0/112 ff0e::
225:1:2:0/112
FTOS(conf-ipv6-acl)#permit ipv6 any ff0e::230:1:2:0/112
FTOS(conf-ipv6-acl)#permit ipv6 165:87:32::0/112 any
FTOS(conf-ipv6-acl)#exit
FTOS(conf)#interface tengigabitethernet 0/84
FTOS(conf-if-te-0/84)#ipv6 pim join-filter JOIN-FIL_ACL in
FTOS(conf-if-te-0/84)#ipv6 pim join-filter JOIN-FIL_ACL out
```

ipv6 pim query-interval

Change the frequency of IPv6 PIM router-query messages.

S5000

Syntax	`ipv6 pim query-interval seconds` To return to the default value, use the `no ipv6 pim query-interval seconds` command.
Parameters	

seconds	Enter a number as the number of seconds between router query messages. The range is 0 to 65535. The default is **30 seconds**.

Defaults	**30 seconds**
Command Modes	INTERFACE
Command History	

Version 9.0(1.3)	Introduced on the S5000.

ipv6 pim neighbor-filter

Prevent the system from forming a PIM adjacency with a neighboring system.

S5000

Syntax	`ipv6 pim neighbor-filter {access-list}`
Parameters	

access-list	Enter the name of a standard access list. Maximum 16 characters.

Defaults	none
Command Modes	CONFIGURATION
Command History	

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	Do not enter this command before creating the access-list.

ipv6 pim register-filter

Configure the source DR so that it does not send register packets to the RP for the specified sources and groups.

S5000

Syntax `ipv6 pim register-filter` *`access-list`*

Parameters

access-list	Enter the name of the extended ACL that contains the sources and groups to be filtered.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf)#ipv6 pim register-filter REG-FIL_ACL
FTOS(conf)#ipv6 access-list REG-FIL_ACL
FTOS(conf-ipv6-acl)#deny ipv6 165:87:34::10/128 ff0e::
225:1:2:0/112
FTOS(conf-ipv6-acl)#permit ipv6 any any
FTOS(conf-ipv6-acl)#exit
```

ipv6 pim rp-address

Configure a static PIM rendezvous point (RP) address for a group. This address is used by first-hop routers to send register packets on behalf of the source multicast host.

S5000

Syntax `ipv6 pim rp-address` *`address`* `group-address` *`group-address mask`* `override`

To remove an RP address, use the `no ipv6 pim re-address` *`address`* `group-address` *`mask`* `override` command.

Parameters

address	Enter the IPv6 RP address in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zero.
group-address ***group-address mask***	Enter the keywords `group-address` followed by the group address in the x:x:x:x::x format and then the mask in /nn format to assign that group address to the RP. **NOTE:** The :: notation specifies successive hexadecimal fields of zero.

override	Enter the keyword `override` to override the BSR updates with static RP. The override takes effect immediately during enable/ disable. **NOTE:** This option is applicable to multicast group range.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The RP addresses are stored in the order in which they are entered. RP addresses learnt via BSR take priority over static RP addresses.

Without the override option, RPs advertised by the BSR updates take precedence over the statically configured RPs.

ipv6 pim rp-candidate

Specify an interface as an RP candidate.

S5000

Syntax

```
ipv6 pim rp-candidate interface-type slot/port [priority-value]
```

Parameters

interface-type slot/port	Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
priority-value	(OPTIONAL) Enter a number as the priority of this RP Candidate, which is included in the Candidate-RP-Advertisements. The range is 0 (highest) to 255 (lowest).

Defaults	none
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ipv6 pim sparse-mode

Enable IPv6 PIM sparse mode on the interface.

S5000

Syntax

`ipv6 pim sparse-mode`

To disable IPv6 PIM sparse mode, use the `no ipv6 pim sparse-mode` command.

Defaults	Disabled.
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	The interface must be enabled (use the `no shutdown` command) and not have the `switchport` command configured. Multicast must also be enabled globally. PIM is supported on the port-channel interface.

ipv6 pim spt-threshold

Specifies when a PIM leaf router should join the shortest path tree.

S5000

Syntax

`ipv6 pim spt-threshold {kbps | infinity}`

To return to the default value, use the `no ipv6 pim spt-threshold` command.

Parameters

kbps	Enter a traffic rate in kilobytes per second. The range is 0 to 4294967 kbps. The default is **10 kbps**.
infinity	Enter the keyword `infinity` to have all sources for the specified group use the shared tree and never join shortest path tree (SPT).

Defaults	**10 kbps**
Command Modes	CONFIGURATION

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Usage Information PIM leaf routers join the shortest path tree immediately after the first packet arrives from a new source.

show ipv6 pim bsr-router

View information on the bootstrap router (v2).

S5000

Syntax `show ipv6 pim bsr-router`

Command Modes

- EXEC
- EXEC Privilege

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ipv6 pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
  BSR address: 14::2
  Uptime: 00:02:54, BSR Priority: 0, Hash mask length: 126
  Next bootstrap message in 00:00:06

This system is a candidate BSR
  Candidate BSR address: 14::2, priority: 0, hash mask length:
126
FTOS#
```

show ipv6 pim interface

Display IPv6 PIM enabled interfaces.

S5000

Syntax `show ipv6 pim interface`

Command Modes

- EXEC
- EXEC Privilege

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ipv6 pim interface
Interface Ver/ Nbr   Query DR
          Mode Count Intvl Prio

Te 10/3   v2/S 1     30    1
  Address : fe80::201:e8ff:fe02:140f
  DR : this router

Te 10/11  v2/S 0     30    1
  Address : fe80::201:e8ff:fe02:1417
  DR : this router
FTOS#
```

show ipv6 pim neighbor

Displays IPv6 PIM neighbor information.

S5000

Syntax

```
show ipv6 pim neighbor [detail]
```

Parameters

detail	(OPTIONAL) Enter the keyword `detail` to displayed PIM neighbor detailed information.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ipv6 pim neighbor detail
Neighbor Interface Uptime/Expires Ver DR
Address                                 Prio/Mode
fe80::201:e8ff:fe00:6265 Te 10/3 00:07:39/00:01:42 v2 1 / S
165:87:50::6
FTOS#
```

show ipv6 pim rp

View all IPv6 multicast groups-to-rendezvous point (RP) mappings.

S5000

Syntax

```
show ipv6 pim rp [mapping | group-address]
```

Parameters

mapping	(OPTIONAL) Enter the keyword `mapping` to display the multicast groups-to-RP mapping and information on how RP is learnt.
group-address	(OPTIONAL) Enter the multicast group address in the x:x:x:x::x format to view RP mappings for a specific group. **NOTE:** The :: notation specifies successive hexadecimal fields of zero.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ipv6 pim rp
Group RP
ff0e::225:1:2:1 14::1
ff0e::225:1:2:2 14::1
ff0e::226:1:2:1 14::1
ff0e::226:1:2:2 14::1
FTOS#
```

Example (Mapping)

```
FTOS#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Group(s): ff00::/8
  RP: 14::1, v2
    Info source: 14::1, via bootstrap, priority 192
         Uptime: 00:03:37, expires: 00:01:53
Group(s): ff00::/8, Static
  RP: 14::2, v2
FTOS#
```

show ipv6 pim tib

View the IPv6 PIM multicast-routing database (tree information base—tib).

S5000

Syntax `show ipv6 pim tib [group-address [source-address]]`

Parameters

group-address	(OPTIONAL) Enter the multicast group address in the x:x:x:x::x format to view RP mappings for a specific group. **NOTE:** The :: notation specifies successive hexadecimal fields of zero.
source-address	(OPTIONAL) Enter the source address in the x:x:x:x::x format.

NOTE: The :: notation specifies successive hexadecimal fields of zero.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show ipv6 pim tib

PIM Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P -
Pruned,
       R - RP-bit set, F - Register flag, T - SPT-bit set, J -
Join SPT,
       M - MSDP created entry, A - Candidate for MSDP
Advertisement
       K - Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(25::1, ff0e::225:1:2:1), uptime 00:09:53, expires
00:00:00,flags: CJ
  RPF neighbor: TenGigabitEthernet 10/3,
fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 10/11

(25::1, ff0e::225:1:2:2), uptime 00:09:54, expires
00:00:00,flags: CJ
  RPF neighbor: TenGigabitEthernet 10/3,
fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 10/11

(25::2, ff0e::225:1:2:2), uptime 00:09:54, expires
00:00:00,flags: CJ
  RPF neighbor: TenGigabitEthernet 10/3,
fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 10/11

(25::1, ff0e::226:1:2:1), uptime 00:09:54, expires
00:00:00,flags: CJ
  RPF neighbor: TenGigabitEthernet 10/3,
fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 10/11
FTOS#
```

40

PIM-Source Specific Mode (PIM-SSM)

FTOS supports protocol-independent multicast (PIM)-source specific mode (PIM-SSM) commands on the S5000.

This chapter contains the following sections:

- IPv4 PIM Commands
- IPv4 PIM-Source Specific Mode Commands
- IPv6 PIM Commands
- IPv6 PIM-Source Specific Mode Commands

IPv4 PIM Commands

The following commands apply to IPv4 PIM-SM, PIM-SSM, and PIM-DM.

- clear ip pim tib
- debug ip pim
- ip pim dr-priority
- ip pim graceful-restart
- ip pim neighbor-filter
- ip pim query-interval
- show ip pim interface
- show ip pim neighbor
- show ip pim tib

IPv4 PIM-Source Specific Mode Commands

The IPv4 PIM-source specific mode (PIM-SSM) commands are as follows.

- ip pim ssm-range
- ip pim join-filter
- show ip pim ssm-range

ip pim ssm-range

Specify the SSM group range using an access list.

S5000

Syntax	`ip pim ssm-range {`*`access_list_name`*`}`
Parameters	***access_list_name*** — Enter the name of the access list.
Defaults	Default SSM range is 232/8 and ff3x/32
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

Usage Information

FTOS supports standard access lists for the SSM range. You cannot use extended ACLs for configuring the SSM range. If you configure an extended ACL and then used in the `ip pim ssm-range {`*`access list name`*`}` configuration, an error is reported.

However, if you configure `ip pim ssm-range {`*`access list name`*`}` first and then you configure the ACL as an Extended ACL, an error is not reported and the ACL is not applied to the SSM range.

FTOS-recommended best-practices are to configure the standard ACL, and then apply the ACL to the SSM range. After the SSM range is applied, the changes are applied internally without requiring clearing of the tree information base (TIB).

When the ACL rules change, the ACL and protocol-independent multicast (PIM) modules apply the new rules automatically.

When you configure the SSM range, FTOS supports SSM for configured group range as well as the default SSM range.

When you remove the SSM ACL, PIM SSM is supported for the default SSM range only.

show ip pim ssm-range

Display the non-default groups added using the SSM range feature.

S5000

Syntax	`show ip pim ssm-range`
Defaults	none
Command Modes	EXEC EXEC Privilege

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

IPv6 PIM Commands

The following commands apply to IPv6 PIM-SM and PIM-SSM.

- clear ipv6 pim tib
- debug ip pim
- ipv6 pim dr-priority
- ipv6 pim join-filter
- ipv6 pim query-interval
- ipv6 pim neighbor-filter
- show ipv6 pim interface
- show ipv6 pim neighbor
- show ipv6 pim tib

IPv6 PIM-Source Specific Mode Commands

The IPv6 PIM-SSM commands are as follows.

- ipv6 pim ssm-range
- show ipv6 pim ssm-range

41

Port Monitoring

The port monitoring feature allows you to monitor network traffic by forwarding a copy of each incoming or outgoing packet from one port to another port.

The commands in this chapter are supported on the S5000.

Important Points to Remember

- Port monitoring is supported on physical ports only. Logical interfaces, such as Port Channels and virtual local area networks (VLANs), are not supported.
- The Dell Networking operating software (FTOS) supports as many monitor sessions on a system as the number of port-pipes.
- The monitoring (destination, “MG”) and monitored (source, “MD”) ports must be on the same switch.
- In general, a monitoring port should have `no ip address` and `no shutdown` as the only configuration; FTOS permits a limited set of commands for monitoring ports; display them using the `?` command. A monitoring port also may not be a member of a VLAN.
- A monitoring port can monitor any physical port in the chassis.
- Only one MG and one MD may be in a single port-pipe.
- A monitoring port can monitor more than one port.
- More than one monitored port can have the same destination monitoring port.
- FTOS on the S5000 supports multiple source ports to be monitored by a single destination port in one monitor session.
- On the S5000, one monitor session can have only one MG port. There is no restriction on the number of source ports, or destination ports on the chassis.

NOTE: The monitoring port should not be a part of any other configuration.

description

Enter a description of this monitoring session.

S5000

Syntax	`description {`*`description`*`}` To remove the description, use the `no description {`*`description`*`}` command.
Parameters	**description** — Enter a description regarding this session (80 characters maximum).

Defaults none

Command Modes MONITOR SESSION (conf-mon-*sess-session-ID*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands monitor session – enables a monitoring session.

monitor session

Create a session for monitoring traffic with port monitoring.

S5000

Syntax `monitor session session-ID`

To delete a session, use the `no monitor session session-ID` command.

To delete all monitor sessions, use the `no monitor session all` command.

Parameters

session-ID	Enter a session identification number. The range is 0 to 65535.

Defaults none

Command Modes MONITOR SESSION (conf-mon-*sess-session-ID*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The `monitor` command is saved in the running configuration at Monitor Session mode level and can be restored after a chassis reload.

Example

```
FTOS(conf)# monitor session 60
FTOS(conf-mon-sess-60)
```

Related Command

show monitor session – displays the monitor session.

show running-config monitor session – displays the running configuration of a monitor session.

show config

Display the current monitor session configuration.

S5000

Syntax `show config`

Defaults	none
Command Modes	MONITOR SESSION (conf-mon-*sess-session-ID*)
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
FTOS(conf-mon-sess-11)#show config
!
monitor session 11
  source TenGigabitEthernet 10/0 destination
TenGigabitEthernet 10/47 direction rx
FTOS#
```

show monitor session

Display the monitor information of a particular session or all sessions.

S5000

Syntax

`show monitor session {session-ID}`

To display monitoring information for all sessions, use the `show monitor session` command.

Parameters

session-ID	(OPTIONAL) Enter a session identification number. The range 0 to 65535.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show monitor session 11
SessionID  Source   Destination    Direction Mode
---------  ------   -------------- --------- -------
11         Te 10/0  Te 10/47       rx        interface
```

Related Commands

monitor session – Creates a session for monitoring.

show running-config monitor session

Display the running configuration of all monitor sessions or a specific session.

S5000

Syntax

`show running-config monitor session {session-ID}`

To display the running configuration for all monitor sessions, use the `show running-config monitor session` command.

Parameters

session-ID	(OPTIONAL) Enter a session identification number. The range 0 to 65535.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `monitoring` command is saved in the running configuration at the Monitor Session mode level and can be restored after a chassis reload.

Example

```
FTOS#show running-config monitor session
!
monitor session 8
  source TenGigabitEthernet 10/46 destination
TenGigabitEthernet 10/1 direction rx
!
monitor session 11
  source TenGigabitEthernet 10/0 destination
TenGigabitEthernet 10/47 direction rx
FTOS#show running-config monitor session 11
!
monitor session 11
  source TenGigabitEthernet 10/0 destination
TenGigabitEthernet 10/47 direction rx
```

Related Commands

monitor session – Creates a session for monitoring.

show monitor session – Displays a monitor session.

source (port monitoring)

Configure a port monitor source.

S5000

Syntax

`source` *`interface`* `destination` *`interface-type slot/port`* `direction {rx | tx | both}`

To disable a monitor source, use the `no source` *`interface-type slot/port`* `destination` *`interface`* `direction {rx | tx | both}` command.

Parameters

interface-type slot/port	Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
destination	Enter the keyword `destination` to indicate the interface destination.
direction {rx | tx | both}	Enter the keyword `direction` followed by one of the packet directional indicators. • `rx`: to monitor receiving packets only. • `tx`: to monitor transmitting packets only. • `both`: to monitor both transmitting and receiving packets.

Defaults

none

Command Modes

MONITOR SESSION (conf-mon-*sess-session-ID*)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-mon-sess-11)#source te 10/0 destination fo 10/47
direction rx
FTOS(conf-mon-sess-11)#
```

42

Per-VLAN Spanning Tree Plus (PVST+)

The Dell Networking operating software (FTOS) implementation of per-VLAN spanning tree plus (PVST+) is based on the IEEE 802.1d standard spanning tree protocol.

PVST+ is supported by FTOS on the S5000 switch.

NOTE: For easier command line entry, the plus (+) sign is not used at the command line.

description

Enter a description of the PVST+.

S5000

Syntax `description {description}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description to identify the spanning tree (80 characters maximum).

Defaults none

Command Modes SPANNING TREE PVST+ (The prompt is "config-pvst".)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands protocol spanning-tree pvst – enter SPANNING TREE mode on the switch.

disable

Disable PVST+ globally.

S5000

Syntax `disable`

To enable PVST+, use the `no disable` command.

Defaults	Disabled.
Command Modes	CONFIGURATION (conf-pvst)
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	protocol spanning-tree pvst – enter PVST+ mode.

extend system-id

Use extend system ID to augment the Bridge ID with a VLAN ID so that PVST+ differentiate between BPDUs for each VLAN. If for some reason on VLAN receives a BPDU meant for another VLAN, PVST+ will then not detect a loop, and both ports can remain in forwarding state.

S5000

Syntax

```
extend system-id
```

Defaults Disabled

Command Modes PROTOCOL PVST

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-pvst)#do show spanning-tree pvst vlan 5 brief
VLAN 5
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32773, Address 0001.e832.73f7
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32773 (priority 32768 sys-id-ext 5),
Address 0001.e832.73f7
We are the root of Vlan 5
Configured hello time 2, max age 20, forward delay 15

Interface Designated
Name    PortID  Prio  Cost   Sts Cost Bridge ID      PortID
-------------------------------------------------------------
Te 0/10 128.140 128  200000 FWD 0   32773 0001.e832.73f7
128.140
Te 0/12 128.142 128  200000 DIS 0   32773 0001.e832.73f7
128.142

Interface
Name     Role PortID  Prio  Cost  Sts Cost Link-type Edge
--------------------------------------------------------
Te 0/10  Desg 128.140 128  200000 FWD 0    P2P       No
Te 0/12  Dis  128.142 128  200000 DIS 0    P2P       No
```

Related Commands protocol spanning-tree pvst – enter SPANNING TREE mode on the switch.

protocol spanning-tree pvst

Enter the PVST+ mode to enable PVST+ on a device.

S5000

Syntax

`protocol spanning-tree pvst`

To disable PVST+, use the `disable` command.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#conf
FTOS(conf)#protocol spanning-tree pvst
FTOS(conf-pvst)#no disable
FTOS(conf-pvst)#vlan 2 bridge-priority 4096
FTOS(conf-pvst)#vlan 3 bridge-priority 16384
FTOS(conf-pvst)#
FTOS(conf-pvst)#show config
!
protocol spanning-tree pvst
  no disable
  vlan 2 bridge-priority 4096
  vlan 3 bridge-priority 16384
FTOS#
```

Usage Information

After you enable PVST+, the device runs an STP instance for each VLAN it supports.

Related Commands

disable – disables PVST+.

show spanning-tree pvst – displays the PVST+ configuration.

show spanning-tree pvst

View the Per-VLAN spanning tree configuration.

S5000

Syntax

show spanning-tree pvst {vlan vlan-id}[interface *type slot/ port*] | [brief] | [guard]

Parameters

vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` followed by the VLAN ID. The range is 1 to 4094.
brief	(OPTIONAL) Enter the keyword `brief` to view a synopsis of the PVST+ configuration information.

interface *type slot/port*	(OPTIONAL) Enter the interface keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
guard	(OPTIONAL) Enter the keyword `guard` to display the type of guard enabled on a PVST interface and the current port state.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output from the `show spanning-tree pvst` command shown in the Examples below.

Interface Name	PVST interface.
Instance	PVST instance.
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard).

Example (Brief)

```
FTOS#show spanning-tree pvst vlan 3 brief
VLAN 3
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 4096, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 16384, Address 0001.e805.e306
Configured hello time 2, max age 20, forward delay 15

Interface                            Designated
Name    PortID  Prio Cost Sts Cost  Bridge ID       PortID
----------------------------------------------------------
Te 1/0  128.130 128 20000 FWD 20000 4096 0001.e801.6aa8
128.426
Te 1/1  128.131 128 20000 BLK 20000 4096 0001.e801.6aa8
128.427
Te 1/16 128.146 128 20000 FWD 20000 16384 0001.e805.e306
128.146
Te 1/17 128.147 128 20000 FWD 20000 16384 0001.e805.e306
128.147

Interface
```

```
Name    Role PortID   Prio Cost  Sts Cost Link-type Edge
-----------------------------------------------------
Te 1/0  Root 128.130  128  20000 FWD 20000 P2P      No
Te 1/1  Altr 128.131  128  20000 BLK 20000 P2P      No
Te 1/16 Desg 128.146  128  20000 FWD 20000 P2P      Yes
Te 1/17 Desg 128.147  128  20000 FWD 20000 P2P      Yes
```

Example

```
FTOS#show spanning-tree pvst vlan 2
VLAN 2
Root Identifier has priority 4096, Address 0001.e805.e306
Root Bridge hello time 2, max age 20, forward delay 15
Bridge Identifier has priority 4096, Address 0001.e805.e306
Configured hello time 2, max age 20, forward delay 15
We are the root of VLAN 2
Current root has priority 4096, Address 0001.e805.e306
Number of topology changes 3, last change occured 00:57:00

Port 130 (TenGigabitEthernet 1/0) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier
128.130
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.130, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1567, received 3
The port is not in the Edge port mode

Port 131 (TenGigabitEthernet 1/1) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier
128.131
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.131, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1567, received 0
The port is not in the Edge port mode

Port 146 (TenGigabitEthernet 1/16) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier
128.146
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.146, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1578, received 0
The port is in the Edge port mode

Port 147 (TenGigabitEthernet 1/17) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier
128.147
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.147, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1579, received 0
The port is in the Edge port mode
```

Example (EDS/ LBK)

```
FTOS#show spanning-tree pvst vlan 2 interface
tengigabitethernet 1/0
```

TenGigabitEthernet 1/0 of VLAN 2 is LBK_INC discarding

```
Edge port:no (default) port guard :none (default)
Link type: point-to-point (auto) bpdu filter:disable (default)
Bpdu guard :disable (default)
Bpdus sent 152, received 27562

Interface Designated
Name    PortID   Prio Cost  Sts Cost Bridge ID       PortID
-----------------------------------------------------------
Te 1/0  128.1223 128  20000 EDS 0 32768 0001.e800.a12b 128.1223
```

Example (EDS/ PVID)

```
FTOS#show spanning-tree pvst vlan 2 interface
tengigabitethernet 1/0
```

TenGigabitEthernet 1/0 of VLAN 2 is PVID_INC discarding

```
Edge port:no (default) port guard :none (default)
Link type: point-to-point (auto) bpdu filter:disable (default)
Bpdu guard :disable (default)
Bpdus sent 1, received 0

Interface Designated
Name   PortID   Prio Cost  Sts Cost Bridge ID       PortID
---------------------------------------------------------
Te 1/0 128.1223 128 20000 EDS 0 32768 0001.e800.a12b 128.1223
```

Example (Guard)

```
FTOS#show spanning-tree pvst vlan 5 guard
Interface
Name   Instance Sts        Guard type
-----------------------------------
Te 0/1 5       INCON(Root) Rootguard
Te 0/2 5       FWD         Loopguard
Te 0/3 5       EDS(Shut)   Bpduguard
```

Related Commands

spanning-tree pvst – configure PVST+ on an interface.

spanning-tree pvst

Configure a PVST+ interface with one of these settings: edge port with optional bridge port data unit (BPDU) guard, port disablement if an error condition occurs, port priority or cost for a VLAN range, loop guard, or root guard.

S5000

Syntax

```
spanning-tree pvst {edge-port [bpduguard [shutdown-on-
violation]] | err-disable | vlan vlan-range {cost number |
priority value} | loopguard | rootguard}
```

Parameters

edge-port	Enter the keywords `edge-port` to configure the interface as a PVST+ edge port.
bpduguard	Enter the keyword `portfast` to enable Portfast to move the interface into Forwarding mode immediately after the root fails. Enter the keyword `bpduguard` to disable the port when it receives a BPDU.

shutdown-on-violation	(OPTIONAL) Enter the keywords `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.
err-disable	Enter the keywords `err-disable` to enable the port to be put into the error-disable state (EDS) if an error condition occurs.
vlan *vlan-range*	Enter the keyword `vlan` followed by the VLAN number(s). The range is 1 to 4094.
cost *number*	Enter the keyword `cost` followed by the port cost value. The range is 1 to 200000. Defaults: • 1-Gigabit Ethernet interface = **20000**. • 10-Gigabit Ethernet interface = **2000**. • 40-Gigabit Ethernet interface = **2000** • Port Channel interface with one 1-Gigabit Ethernet = **20000**. • Port Channel interface with one 10-Gigabit Ethernet = **2000**. • Port Channel interface with one 40-Gigabit Ethernet = **2000**. • Port Channel with two 1-Gigabit Ethernet = **18000**. • Port Channel with two 10-Gigabit Ethernet = **1800**. • Port Channel with two 40-Gigabit Ethernet = **1800**.
priority *value*	Enter the keyword `priority` followed the Port priority value in increments of 16. The range is 0 to 240. The default is **128**.
loopguard	Enter the keyword `loopguard` to enable loop guard on a PVST+ port or port-channel interface.
rootguard	Enter the keyword `rootguard` to enable root guard on a PVST+ port or port-channel interface.

Defaults Not configured.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The BPDU guard option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, or is misconfigured, or is subject to a DOS attack. This option places the port into an the Error Disable state if a BPDU appears, and a message is logged so that the administrator can take corrective action.

> **NOTE:** A port configured as an edge port, on a PVST switch, immediately transitions to the forwarding state. Only ports connected to end-hosts should be configured as an edge port. Consider an edge port similar to a port with a spanning-tree portfast enabled.

If you do not enable `shutdown-on-violation`, BPDUs are still sent to the stack-unit CPU.

You cannot enable `root guard` and `loop guard` at the same time on a port. For example, if you configure `loop guard` on a port on which `root guard` is already configured, the following error message is displayed: `% Error: RootGuard is configured. Cannot configure LoopGuard`.

When used in a PVST+ network, loop guard is performed per-port or per-port channel at a VLAN level. If no BPDUs are received on a VLAN interface, the port or port-channel transitions to a Loop-Inconsistent (blocking) state only for this VLAN.

Enabling Portfast BPDU guard and loop guard at the same time on a port results in a port that remains in a Blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an Err-Disabled Blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a Loop-Inconsistent Blocking state and no traffic is forwarded on the port.

Example

```
FTOS(conf-if-te-1/1)#spanning-tree pvst vlan 3 cost 18000
FTOS(conf-if-te-1/1)#end
FTOS(conf-if-te-1/1)#show config
!
interface TenGigabitEthernet 1/1
  no ip address
  switchport
  spanning-tree pvst vlan 3 cost 18000
  no shutdown
FTOS(conf-if-te-1/1)#end

FTOS#
```

Related Commands

show spanning-tree pvst – views the PVST+ configuration.

spanning-tree pvst err-disable

Place ports in an Err-Disabled state if they receive a PVST+ BPDU when they are members an untagged VLAN.

S5000

Syntax

`spanning-tree pvst err-disable cause invalid-pvst-bpdu`

Defaults

Enabled; ports are placed in the Err-Disabled state if they receive a PVST+ BPDU when they are members of an untagged VLAN.

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Some non-Dell Networking systems which have hybrid ports participating in PVST+ transmit two kinds of BPDUs: an 802.1D BPDU and an untagged PVST+ BPDU.

Dell Networking systems do not expect PVST+ BPDU on an untagged port. If this happens, FTOS places the port in the Error-Disable state. This behavior might result in the network not converging. To prevent FTOS from executing this action, use the `no spanning-tree pvst err-disable` command cause `invalid-pvst-bpdu`.

Related Commands	show spanning-tree pvst – views the PVST+ configuration.

tc-flush-standard

Enable MAC address flushing after receiving every topology change notification.

S5000

Syntax	`tc-flush-standard` To disable, use the `no tc-flush-standard` command.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	By default, FTOS implements an optimized flush mechanism for PVST+. This helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, you can turn this *knob* command on to enable flushing MAC addresses after receiving every topology change notification.

vlan bridge-priority

Set the PVST+ bridge-priority for a VLAN or a set of VLANs.

S5000

Syntax	`vlan vlan-range bridge-priority value` To return to the default value, use the `no vlan bridge-priority` command.

Parameters

vlan *vlan-range*	Enter the keyword `vlan` followed by the VLAN number(s). The range is 1 to 4094.
bridge-priority *value*	Enter the keywords `bridge-priority` followed by the bridge priority value in increments of 4096. The range is 0 to 61440. The default is **32768**.

Defaults	**32768**
Command Modes	CONFIGURATION (conf-pvst)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

vlan forward-delay – changes the time interval before FTOS transitions to the Forwarding state.

vlan hello-time – change the time interval between BPDUs.

vlan max-age – changes the time interval before PVST+ refreshes.

show spanning-tree pvst – displays the PVST+ configuration.

vlan forward-delay

Set the amount of time the interface waits in the Listening state and the Learning state before transitioning to the Forwarding state.

S5000

Syntax

`vlan vlan-range forward-delay seconds`

To return to the default setting, use the `no vlan forward-delay` command.

Parameters

vlan *vlan-range*	Enter the keyword `vlan` followed by the VLAN number(s). The range is 1 to 4094.
forward-delay *seconds*	Enter the keywords `forward-delay` followed by the time interval, in seconds, that FTOS waits before transitioning PVST+ to the forwarding state. The range is 4 to 30 seconds. The default is **15 seconds**.

Defaults **15 seconds**

Command Modes CONFIGURATION (conf-pvst)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

vlan bridge-priority – sets the bridge-priority value.

vlan hello-time – changes the time interval between BPDUs.

vlan max-age – changes the time interval before PVST+ refreshes.

show spanning-tree pvst – displays the PVST+ configuration.

vlan hello-time

Set the time interval between generation of PVST+ 7 BPDUs.

S5000

Syntax

`vlan vlan-range hello-time seconds`

To return to the default value, use the `no vlan hello-time` command.

Parameters

vlan *vlan-range*	Enter the keyword `vlan` followed by the VLAN number(s). The range is 1 to 4094.
hello-time *seconds*	Enter the keywords `hello-time` followed by the time interval, in seconds, between transmission of BPDUs. The range is 1 to 10 seconds. The default is **2 seconds**.

Defaults

2 seconds

Command Modes

CONFIGURATION (conf-pvst)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

vlan bridge-priority – sets the bridge-priority value.

vlan forward-delay – changes the time interval before FTOS transitions to the forwarding state.

vlan max-age – changes the time interval before PVST+ refreshes.

show spanning-tree pvst – displays the PVST+ configuration.

vlan max-age

Set the time interval for the PVST+ bridge to maintain configuration information before refreshing that information.

S5000

Syntax

`vlan vlan-range max-age seconds`

To return to the default, use the `no vlan max-age` command.

Parameters

vlan *vlan-range*	Enter the keyword `vlan` followed by the VLAN number(s). The range is 1 to 4094.
max-age *seconds*	Enter the keywords `max-age` followed by the time interval, in seconds, that FTOS waits before refreshing configuration information. The range is 6 to 40 seconds. The default is **20 seconds**.

Defaults

20 seconds

Command Modes CONFIGURATION (conf-pvst)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

vlan bridge-priority – sets the bridge-priority value.

vlan forward-delay – changes the time interval before FTOS transitions to the forwarding state.

vlan hello-time – changes the time interval between BPDUs.

show spanning-tree pvst – displays the PVST+ configuration.

43

Quality of Service (QoS)

The Dell Networking operating software (FTOS) commands for quality of service (QoS) include traffic conditioning and congestion control. QoS commands are supported on the S500 switch.

This chapter contains the following sections:

- Global Configuration Commands
- Per-Port QoS Commands
- Policy-Based QoS Commands

Global Configuration Commands

There is only one global configuration QoS command.

qos-rate-adjust

By default, while rate limiting, policing, and shaping, FTOS does not include the Preamble, SFD, or the IFG fields. These fields are overhead; only the fields from MAC destination address to the CRC are used for forwarding and are included in these rate metering calculations. You can optionally include overhead fields in rate metering calculations by enabling QoS Rate Adjustment.

S5000

Syntax `qos-rate-adjustment` *`overhead-bytes`*

Parameters

overhead-bytes	Include a specified number of bytes of packet overhead to include in rate limiting, policing, and shaping calculations. The range is 1 to 31.

Defaults QoS rate adjustment is disabled by default, and `no qos-rate-adjust` is listed in the running-configuration

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Per-Port QoS Commands

Per-port QoS (port-based QoS) allows you to define the QoS configuration on a per-physical-port basis.

dot1p-priority

Assign a value to the IEEE 802.1p bits on the traffic received by this interface.

S5000

Syntax `dot1p-priority priority-value`

To delete the IEEE 802.1p configuration on the interface, use the `no dot1p-priority` command.

Defaults Enter a value from 0 to 7.

Table 9. Priority Values for 802.1p Traffic

dot1p Priority Value	Queue ID
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

For the S5000, enter a value 0, 2, 4, or 6.

Defaults none

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The `dot1p-priority` command changes the priority of incoming traffic on the interface. The system places traffic marked with a priority in the correct queue and processes that traffic according to its queue.

When you set the priority for a port channel, the physical interfaces assigned to the port channel are configured with the same value. You cannot assign the `dot1p-priority` command to individual interfaces in a port channel.

rate police

Police the incoming traffic rate on the selected interface.

S5000

Syntax

```
rate police [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB]] [vlan vlan-id]
```

Parameters

kbps	Enter the keyword `kbps` to specify the rate limit in Kilobits per second (Kbps). Specify a value after the keyword as a multiple of 64.
committed-rate	Enter the bandwidth in Mbps. The range is 0 to 10000.
burst-KB	(OPTIONAL) Enter the burst size in KB. The range is 16 to 200000. The default is **50**.
peak *peak-rate*	(OPTIONAL) Enter the keyword `peak` followed by a number to specify the peak rate in Mbps. The range is 0 to 10000.
vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` followed by a VLAN ID to police traffic to those specific VLANs. The range is 1 to 4094.

Defaults

Granularity for `commited-rate` and `peak-rate` is Mbps unless you use the `kbps` option.

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

NOTE: Per Port rate limit and rate police is supported for Layer 2 tagged and untagged switched traffic and for Layer 3 traffic. Per VLAN rate limit and rate police is supported on only tagged ports with Layer 2 switched traffic.

On one interface, you can configure the `rate police` command for a VLAN or you can configure the `rate police` command for an interface. For each physical interface, you can configure three `rate police` commands specifying different VLANS.

For each physical interface, you can configure six `rate police` commands specifying different VLANS.

After configuring VLANs in the `rate police` command, if this error message appears: `%Error: Specified VLANs overlap with existing config.` check to see if the same VLANs are used with the `rate limit` command on other interfaces. To clear the problem, remove the `rate limit` configuration(s), and re-configure the `rate police` command. After the `rate police` command is configured, return to the other interfaces and re-apply the `rate limit` configuration.

Related Commands

rate-police – specifies traffic policing on the selected interface.

rate shape

Shape the traffic output on the selected interface.

S5000

Syntax	`rate shape [kbps] rate [burst-KB]`
Parameters	**kbps** — Enter the keyword `kbps` to specify the rate limit in Kilobits per second (Kbps). Specify a value after the keyword as a multiple of 64. *rate* — Enter the outgoing rate in multiples of 10 Mbps. The range is 10 to 10000. *burst-KB* — (OPTIONAL) Enter the burst size in KB. The range is 0 to 10000. The default is **10**.
Defaults	Granularity for rate is **Mbps** unless you use the `kbps` option.
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** — Introduced on the S5000.
Related Commands	rate-shape – shapes traffic output as part of the designated policy.

service-class dot1p-mapping

Configure a service-class criterion based on a dot1p value.

S5000

Syntax

```
service-class dot1p-mapping {dot1p0 value | dot1p1 value |
dot1p2 value | dot1p3 value | dot1p4 value| dot1p5 value |
dot1p6 value | dot1p7 value}
```

Parameters

dot1p0 *value* ... **dot1p7** *value*	Enter a dot1p list number and value. The list number range is 0 to 7. The range is 0 to 3.

Defaults

For each dot1p Priority, the default CoS queue value is:

- dot1p Priority: 0 1 2 3 4 5 6 7
- CoS Queue: 0 0 0 1 2 3 3 3

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To apply dot1p-queue-mapping, use the `service-class dynamic dot1p` command.

Related Commands

show qos dot1p-queue-mapping – displays the dot1p priority to queue mapping on the switch.

service-class dynamic dot1p

Honor all 802.1p markings on incoming switched traffic on an interface (from INTERFACE mode) or on all interfaces (from CONFIGURATION mode). A CONFIGURATION mode entry supersedes an INTERFACE mode entries.

S5000

Syntax

`service-class dynamic dot1p`

To return to the default setting, use the `no service-class dynamic dot1p` command.

Defaults

All dot1p traffic is mapped to Queue 0 unless you enable the `service-class dynamic dot1p` command. The default mapping is as follows:

Table 10. Default Mapping for 802.1p Traffic

dot1p Priority Value	Queue ID
0	0
1	0
2	0
3	1
4	2
5	3
6	3
7	3

Command Modes

- INTERFACE
- CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Enter this command to honor all incoming 802.1p markings on incoming switched traffic on the interface. By default, this facility is not enabled (that is, the 802.1p markings on incoming traffic are not honored).

You can apply this command on both physical interfaces and port channels. When you set the service-class dynamic for a port channel, the physical interfaces assigned to the port channel are automatically configured; you cannot assign the `service-class dynamic` command to individual interfaces in a port channel.

All traffic is by default mapped to the same queue, Queue 0. If you honor dot1p on ingress, you can create service classes based the queueing strategy using the `service-class dynamic dot1p` command from INTERFACE mode. You may apply this queuing strategy to all interfaces by entering this command from CONFIGURATION mode.

- All dot1p traffic is mapped to Queue 0 unless you enble the `service-class dynamic dot1p` command on an interface or globally.
- Layer 2 or Layer 3 service policies supercede dot1p service classes.

service-class bandwidth-weight

Specify a minimum bandwidth for queues.

S5000

Syntax

`service-class bandwidth-weight queue0 *number* queue1 *number* queue2 *number* queue3 *number*`

Parameters

number	Enter the bandwidth-weight. The value must be a power of 2. The range is 1 to 1024.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Guarantee a minimum bandwidth to different queues globally using the `service-class bandwidth-weight` command from CONFIGURATION mode. The command is applied in the same way as the `bandwidth-weight` command in an output QoS policy. The `bandwidth-weight` command in QOS-POLICY-OUT mode supercedes the `service-class bandwidth-weight` command.

strict-priority queue

Configure a unicast queue as a strict-priority (SP) queue.

S5000

Syntax

`strict-priority queue unicast *number*`

Parameters

unicast *number*	Enter the keyword `unicast` followed by the queue number. The range is 1 to 3.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

After you configure a unicast queue as strict-priority, that particular queue, on the entire chassis, is treated as a `strict-priority queue`. Traffic for a strict priority is scheduled before any other queues are serviced. For example, if you send 100% line rate traffic over the SP queue, it starves all other queues on the ports on which this traffic is flowing.

Policy-Based QoS Commands

Policy-based traffic classification is handled with class maps. These maps classify unicast traffic into one of four classes on the S5000. FTOS allows you to match multiple class maps and specify multiple match criteria. Policy-based QoS is not supported on logical interfaces, such as port-channels, VLANs, or loopbacks.

bandwidth-percentage

Assign a percentage of weight to the class/queue.

S5000

Syntax `bandwidth-percentage` *`percentage`*

To remove the bandwidth percentage, use the `no bandwidth-percentage` command.

Parameters

percentage	Enter the percentage assignment of weight to the class/queue. The range is 0 to 100% (granularity 1%).

Defaults none

Command Modes CONFIGURATION (conf-qos-policy-out)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The unit of bandwidth percentage is 1%. A bandwidth percentage of 0 is allowed and disables the scheduling of that class. If the sum of the bandwidth percentages given to all eight classes exceeds 100%, the bandwidth percentage automatically scales down to 100%.

Related Commands	qos-policy-output – creates a QoS output policy.

class-map

Create/access a class map. Class maps differentiate traffic so that you can apply separate quality of service policies to each class.

S5000

Syntax `class-map {match-all | match-any} class-map-name [layer2]`

Parameters

match-all	Determines how packets are evaluated when multiple match criteria exist. Enter the keywords `match-all` to determine that the packets must meet all the match criteria in order to be considered a member of the class.
match-any	Determines how packets are evaluated when multiple match criteria exist. Enter the keywords `match-any` to determine that the packets must meet at least one of the match criteria in order to be considered a member of the class.
class-map-name	Enter a name of the class for the class map in a character format (32 character maximum).
layer2	Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is **Layer 3**.

Defaults Layer 3

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Packets arriving at the input interface are checked against the match criteria and configured using this command to determine if the packet belongs to that class. This command accesses CLASS-MAP mode, where the configuration commands include the`match ip` and `match mac` options.

Related Commands

ip access-list extended – configures an extended IP ACL.

ip access-list standard – configures a standard IP ACL.

match ip access-group – configures the match criteria based on the access control list (ACL).

match ip precedence – identifies the IP precedence values as match criteria.

match ip dscp – configures the match criteria based on the DSCP value.

match mac access-group – configures a match criterion for a class map based on the contents of the designated MAC ACL.

match mac dot1p – configures a match criterion for a class map based on a dot1p value.

match mac vlan – configures a match criterion for a class map based on VLAN ID.

service-queue – assigns a class map and QoS policy to different queues.

show qos class-map – views the current class map information.

clear qos statistics

Clears Matched Packets, Matched Bytes, and Dropped Packets.

S5000

Syntax `clear qos statistics interface` *`type slot/port`*

Parameters

interface ***type slot/port***	Enter the `interface` keyword followed by interface type and slot/ port number. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands show qos statistics – displays the QoS statistics.

description

Add a description to the selected policy map or QoS policy.

S5000

Syntax `description {`*`description`*`}`

To remove the description, use the `no description {`*`description`*`}` command.

Parameters

description	Enter a description to identify the policies (80 characters maximum).

Defaults

none

Command Modes

CONFIGURATION (policy-map-input and policy-map-output; conf-qos-policy-in and conf-qos-policy-out; wred)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

policy-map-input – creates an input policy map.

policy-map-output – creates an output policy map.

qos-policy-input – creates an input QoS-policy on the router.

qos-policy-output – creates an output QoS-policy on the router.

wred-profile – creates a WRED profile.

match ip access-group

Configure match criteria for a class map, based on the access control list (ACL).

S5000

Syntax

```
match ip access-group access-group-name [set-ip-dscp value]
```

To remove ACL match criteria from a class map, use the `no match ip access-group access-group-name [set-ip-dscp value]` command.

Parameters

access-group-name	Enter the ACL name whose contents are used as the match criteria in determining if packets belong to the class specified by class-map.
set-ip-dscp *value*	(OPTIONAL) Enter the keywords `set-ip-dscp` followed by the IP DSCP value. The matched traffic is marked with the DSCP value. The range is 0 to 63.

Defaults

none

Command Modes

CLASS-MAP CONFIGURATION (config-class-map)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must enter the `class-map` command in order to access this command. After the class map is identified, you can configure the match criteria. For class-map match-any, a maximum of five ACL match criteria are allowed. For `class-map match-all`, only one ACL match criteria is allowed.

Related Commands

class-map – identifies the class map.

match ip dscp

Use a differentiated services code point (DSCP) value as a match criteria.

S5000

Syntax

```
match ip dscp dscp-list
```

To remove a DSCP value as a match criteria, use the `no match ip dscp dscp-list` command.

Parameters

dscp-list	Enter the IP DSCP value(s) that is to be the match criteria. Separate values by commas — no spaces (1,2,3) or indicate a list of values separated by a hyphen (1-3). The range is 0 to 63.

Defaults none

Command Modes CLASS-MAP CONFIGURATION (config-class-map)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must enter the `class-map` command in order to access this command. After the class map is identified, you can configure the match criteria.

The `match ip dscp` and `match ip precedence` commands are mutually exclusive.

Up to 64 IP DSCP values can be matched in one match statement. For example, to indicate IP DCSP values 0 1 2 3 4 5 6 7, enter either the `match ip dscp 0,1,2,3,4,5,6,7` or `match ip dscp 0-7` command.

NOTE: Only one of the IP DSCP values must be a successful match criterion, not all of the specified IP DSCP values need to match.

Related Commands

class-map – identifies the class map.

match ip precedence

Use IP precedence values as a match criteria.

S5000

Syntax

```
match ip precedence ip-precedence-list [set-ip-dscp value]
```

To remove IP precedence as a match criteria, use the `no match ip precedence ip-precedence-list [set-ip-dscp value]` command.

Parameters

ip-precedence-list	Enter the IP precedence value(s) as the match criteria. Separate values by commas — no spaces (1,2,3) or indicate a list of values separated by a hyphen (1-3). The range is 0 to 7.

set-ip-dscp *value*	(OPTIONAL) Enter the keywords `set-ip-dscp` followed by the IP DSCP value. The matched traffic is marked with the DSCP value. The range is 0 to 63.

Defaults none

Command Modes CLASS-MAP CONFIGURATION (config-class-map)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must enter the `class-map` command in order to access this command. After the class map is identified, you can configure the match criteria.

The `match ip precedence` command and the `match ip dscp` command are mutually exclusive.

Up to eight precedence values can be matched in one match statement. For example, to indicate the IP precedence values 0 1 2 3, enter either the `match ip precedence 0-3` or `match ip precedence 0,1,2,3` command.

NOTE: Only one of the IP precedence values must be a successful match criterion, not all of the specified IP precedence values need to match.

Related Commands

class-map – identifies the class map.

match mac access-group

Configure a match criterion for a class map, based on the contents of the designated MAC ACL.

S5000

Syntax

`match mac access-group {`*`mac-acl-name`*`}`

Parameters

mac-acl-name	Enter a MAC ACL name. Its contents is used as the match criteria in the class map.

Defaults none

Command Modes CLASS-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must enter the `class-map` command in order to access this command. After the class map is identified, you can configure the match criteria.

Related Commands

class-map – identifies the class map.

match mac dot1p

Configure a match criterion for a class map based on a dot1p value.

S5000

Syntax `match mac dot1p {dot1p-list}`

Parameters

dot1p-list	Enter a dot1p value. The range is 0 to 7.

Defaults none

Command Modes CLASS-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information You must enter the `class-map` command in order to access this command. After the class map is identified, you can configure the match criteria.

Related Commands class-map – identifies the class map.

match mac vlan

Configure a match criterion for a class map based on VLAN ID.

S5000

Syntax `match mac vlan number`

Parameters

number	Enter the VLAN ID. The range is 1 to 4094.

Defaults none

Command Modes CLASS-MAP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information You must enter the `class-map` command in order to access this command. You can match against only one VLAN ID.

Related Commands class-map – identifies the class map.

policy-aggregate

Allow an aggregate method of configuring per-port QoS via policy maps. An aggregate QoS policy is part of the policy map (input/output) applied on an interface.

S5000

Syntax `policy-aggregate` *`qos-policy-name`*

To remove a policy aggregate configuration, use the `no policy-aggregate` *`qos-policy-name`* command.

Parameters

qos-policy-name	Enter the name of the policy map in character format (32 characters maximum).

Defaults none

Command Modes CONFIGURATION (policy-map-input and policy-map-output)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Aggregate input/output QoS policy applies to all the port ingoing/outgoing traffic. Aggregate input/output QoS policy can coexist with per queue input/output QoS policies.

1. If only aggregate input QoS policy exists, input traffic conditioning configurations (rate-police) apply. Any marking configurations in aggregate input QoS policy are ignored.
2. If aggregate input QoS policy and per class input QoS policy coexist, aggregate input QoS policy preempts per class input QoS policy on input traffic conditioning (rate-police). In other words, if rate police configuration exists in the aggregate QoS policy, the rate police configurations in per class QoS are ignored. Marking configurations in per class input QoS policy still apply to each queue.

Related Commands

policy-map-input – creates an input policy map.

policy-map-input

Create an input policy map.

S5000

Syntax `policy-map-input` *`policy-map-name`* `[layer2]`

To remove an input policy map, use the `no policy-map-input` *`policy-map-name`* `[layer2]` command.

Parameters

policy-map-name	Enter the name of the policy map in character format (32 characters maximum).

layer2	(OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is **Layer 3**.

Defaults Layer 3

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The input policy map is used to classify incoming traffic to different flows using class-map, QoS policy, or incoming packets DSCP. This command enables Policy-Map-Input Configuration mode (conf-policy-map-in).

Related Commands

service-queue – assigns a class map and QoS policy to different queues.

policy-aggregate – allows an aggregate method of configuring per-port QoS using policy maps.

service-policy input – applies an input policy map to the selected interface.

policy-map-output

Create an output policy map.

S5000

Syntax `policy-map-output` *`policy-map-name`*

To remove a policy map, use the `no policy-map-output` *`policy-map-name`* command.

Parameters

policy-map-name	Enter the name for the policy map in character format (16 characters maximum).

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The output policy map is used to assign traffic to different flows using QoS policy. This command enables Policy-Map-Output Configuration mode (conf-policy-map-out).

Related Commands

service-queue – assigns a class map and QoS policy to different queues.

policy-aggregate – allows an aggregate method of configuring per-port QoS using policy maps.

service-policy output – applies an output policy map to the selected interface.

qos-policy-input

Create a QoS input policy on the router.

S5000

Syntax

`qos-policy-input` *`qos-policy-name`* `[layer2]`

To remove an existing input QoS policy from the router, use the `no qos-policy-input` *`qos-policy-name`* `[layer2]` command.

Parameters

qos-policy-name	Enter the name for the policy map in character format (32 characters maximum).
layer2	(OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is **Layer 3**.

Defaults

Layer 3

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use this command to specify the name of the input QoS policy. After the input policy is specified, rate-police can be defined. This command enables Qos-Policy-Input Configuration mode— (conf-qos-policy-in).

When changing a Service-Queue configuration in a QoS policy map, all QoS rules are deleted and re-added automatically to ensure that the order of the rules is maintained. As a result, the Matched Packets value shown in the `show qos statistics` command is reset.

Related Commands

rate police – incoming traffic policing function.

qos-policy-output

Create a QoS output policy.

S5000

Syntax

`qos-policy-output` *`qos-policy-name`*

To remove an existing output QoS policy, use the `no qos-policy-output` *`qos-policy-name`* command.

Parameters

qos-policy-name	Enter your output QoS policy name in character format (32 characters maximum).

Defaults	none
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Use this command to specify the name of the output QoS policy. After specifying the output policy, you can define rate-limit and bandwidth-percentage. This command enables Qos-Policy-Output Configuration mode—(conf-qos-policy-out). When changing a service-queue configuration in a QoS policy map, all QoS rules are deleted and re-added automatically to ensure that the order of the rules is maintained. As a result, the Matched Packets value shown in the `show qos statistics`command is reset.
Related Commands	rate limit – outgoing traffic rate-limit functionality. bandwidth-percentage – assigns weight to the class/queue percentage. bandwidth-weight – assigns a priority weight to a queue.

rate-police

Specify the policing functionality on incoming traffic.

S5000

Syntax

```
rate-police [kbps] committed-rate [burst-KB] [peak [kbps] peak-
rate [burst-KB]]
```

Parameters

kbps	Enter the keyword `kbps` to specify the rate limit in Kilobits per second (Kbps). Specify a value after the keyword as a multiple of 64.
committed-rate	Enter the bandwidth in Mbps. The range is 0 to 10000.
burst-KB	(OPTIONAL) Enter the burst size in KB. The range is 16 to 200000. The default is **50**.
peak *peak-rate*	(OPTIONAL) Enter the keyword `peak` followed by a number to specify the peak rate in Mbps. The range is 0 to 10000. The default is the same as designated for `committed-rate`.

Defaults	Burst size is 50 KB. `peak-rate` is by default the same as `committed-rate`. Granularity for `committed-rate` and `peak-rate` is Mbps unless you use the `kbps` option.
Command Modes	QOS-POLICY-IN
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	rate police – specifies traffic policing on the selected interface.

qos-policy-input – creates a QoS output policy.

rate-shape

Shape traffic output as part of the designated policy.

S5000

Syntax `rate-shape [kbps] rate [burst-KB]`

Parameters

kbps	Enter the keyword `kbps` to specify the rate limit in Kilobits per second (Kbps). Specify a value after the keyword as a multiple of 64.
rate	Enter the outgoing rate in multiples of 10 Mbps. The range is 10 to 10000.
burst-KB	(OPTIONAL) Enter the burst size in KB. The range is 0 to 10000. The default is **10**.

Defaults Burst size is 10 KB. Granularity for rate is Mbps unless you use the `kbps` option.

Command Modes QOS-POLICY-OUT

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information `rate-shape` can be applied only as an aggregate policy. If it is applied as a class-based policy, rate-shape does not take effect.

Related Commands

rate shape – shapes traffic output as part of the designated policy.

qos-policy-output – creates a QoS output policy.

service-policy input

Apply an input policy map to the selected interface.

S5000

Syntax `service-policy input policy-map-name [layer2]`

To remove the input policy map from the interface, use the `no service-policy input policy-map-name [layer2]` command.

Parameters

policy-map-name	Enter the name for the policy map in character format (16 characters maximum). You can identify an existing policy map or name one that does not yet exist.

layer2	(OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is **Layer 3**.

Defaults **Layer 3**

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information You can attach a single policy-map to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.

NOTE: The `service-policy` commands are not allowed on a port channel. The `service-policy input policy-map-name` command and the `service-class dynamic dot1p` command are not allowed simultaneously on an interface. However, the `service-policy input` command (without the `policy-map-name` option) and the `service-class dynamic dot1p` command are allowed on an interface.

Related Commands policy-map-input – creates an input policy map.

service-policy output

Apply an output policy map to the selected interface.

S5000

Syntax `service-policy output` *`policy-map-name`*

To remove the output policy map from the interface, use the `no service-policy output` *`policy-map-name`* command.

Parameters

policy-map-name	Enter the name for the policy map in character format (16 characters maximum). You can identify an existing policy map or name one that does not yet exist.

Defaults none

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information A single policy-map can be attached to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.

Related Commands policy-map-output – creates an output policy map.

service-queue

Assign a class map and QoS policy to different queues.

S5000

Syntax

`service-queue` *`queue-id`* `[class-map` *`class-map-name`*`] [qos-policy` *`qos-policy-name`*`]`

To remove the queue assignment, use the `no service-queue` *`queue-id`* `[class-map` *`class-map-name`*`] [qos-policy` *`qos-policy-name`*`]` command.

Parameters

queue-id	Enter the value used to identify a queue. The range is 0 to 3 (four queues per interface; four queues are reserved for control traffic).
class-map *class-map-name*	(OPTIONAL) Enter the keyword `class-map` followed by the class map name assigned to the queue in character format (16 character maximum). **NOTE:** This option is available under `policy-map-input` only.
qos-policy *qos-policy-name*	(OPTIONAL) Enter the keywords `qos-policy` followed by the QoS policy name assigned to the queue in text format (16 characters maximum). This specifies the input QoS policy assigned to the queue under `policy-map-input` and output QoS policy under `policy-map-output` context.

Defaults

none

Command Modes

CONFIGURATION (conf-policy-map-in and conf-policy-map-out)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

There are eight four (4) queues per interface on the S5000. This command assigns a class map or QoS policy to different queues.

Related Commands

class-map – identifies the class map.

service-policy input – applies an input policy map to the selected interface.

service-policy output – applies an output policy map to the selected interface.

set

Mark outgoing traffic with a differentiated service code point (DSCP) or dot1p value.

S5000

Syntax

`set {ip-dscp` *`value`* `| mac-dot1p` *`value`*`}`

Parameters

ip-dscp ***value***	(OPTIONAL) Enter the keywords `ip-dscp` followed by the IP DSCP value. The range is 0 to 63.
mac-dot1p ***value***	Enter the keywords `mac-dot1p` followed by the dot1p value. On theS5000, the allowed values are: 0, 2, 4, 6.

Defaults none

Command Modes CONFIGURATION (conf-qos-policy-in)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information After the IP DSCP bit is set, other QoS services can then operate on the bit settings.

show qos class-map

View the current class map information.

S5000

Syntax `show qos class-map [class-name]`

Parameters

class-name	(Optional) Enter the name of a configured class map.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show qos class-map

Class-map match-any CM
  Match ip access-group ACL
```

Related Commands class-map – identifies the class map.

show qos dot1p-queue-mapping

Displays the dot1p priority to queue mapping on the switch.

S5000

Syntax	`show qos dot1p-queue-mapping`
Defaults	• dot1p Priority: 0 1 2 3 4 5 6 7 • Queue: 0 0 0 1 2 3 3 3
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	service-class dot1p-mapping – Identifies the class map.

show qos policy-map

View the QoS policy map information.

S5000

Syntax

```
show qos policy-map {summary [interface] | detail [interface]}
```

Parameters

summary ***interface***	To view a policy map interface summary, enter the keyword `summary` and optionally one of the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
detail ***interface***	To view a policy map interface in detail, enter the keyword `detail` and optionally one of the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (IPv4)

```
FTOS#show qos policy-map detail tengigabitethernet 0/0

Interface TenGigabitEthernet 4/1

Policy-map-input policy
Trust diffserv
Queue# Class-map-name Qos-policy-name
 0 - q0
 1 CM1q1
 2 CM2q2
 3 CM3q3
 4 CM4q4
 5 CM5q5
 6 CM6q6
 7 CM7q7
FTOS#
```

Example (IPv6)

```
FTOS# show qos policy-map detail tengigabitethernet 0/0

Interface TenGigabitEthernet 8/29

Policy-map-input pmap1
Trust ipv6-diffserv
Queue# Class-map-name Qos-policy-name
 0       c0            q0
 1       c1            q1
 2       c2            q2
 3       c3            q3
 4       c4            q4
 5       c5            -
 6       c6            q6
 7       c7            q7
FTOS#
```

Example (Summary IPv4)

```
FTOS#sho qos policy-map summary

Interface policy-map-input policy-map-output
Te 4/1     PM1                 -
Te 4/2     PM2        PMOut
FTOS#
```

show qos policy-map-input

View the input QoS policy map details.

S5000

Syntax

```
show qos policy-map-input [policy-map-name] [class class-map-
name] [qos-policy-input qos-policy-name]
```

Parameters

policy-map-name	Enter the policy map name.
class *class-map-name*	Enter the keyword `class` followed by the class map name.
qos-policy-input *qos-policy-name*	Enter the keyword `qos-policy-input` followed by the QoS policy name.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show qos policy-map-input

Policy-map-input PolicyMapInput
Aggregate Qos-policy-name AggPolicyIn
Queue# Class-map-name  Qos-policy-name
0      ClassMap1       qosPolicyInput
FTOS#
```

Example

```
FTOS# show qos policy-map-input

Policy-map-input pmap1
Trust ipv6-diffserv
Queue#  Class-map-name  Qos-policy-name
0       c0              q0
1       c1              q1
2       c2              q2
3       c3              q3
4       c4              q4
5       c5              -
6       c6              q6
7       c7              q7
FTOS#
```

show qos policy-map-output

View the output QoS policy map details.

S5000

Syntax

`show qos policy-map-output [`*`policy-map-name`*`] [qos-policy-output `*`qos-policy-name`*`]`

Parameters

policy-map-name	Enter the policy map name.
qos-policy-output *qos-policy-name*	Enter the keyword `qos-policy-output` followed by the QoS policy name.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show qos policy-map-output

Policy-map-output PolicyMapOutput
Aggregate Qos-policy-name AggPolicyOut
Queue#   Qos-policy-name
  0      qosPolicyOutput
FTOS#
```

show qos qos-policy-input

View the input QoS policy details.

S5000

Syntax

`show qos qos-policy-input [`*`qos-policy-name`*`]`

Parameters

qos-policy-name	Enter the QoS policy name.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show qos qos-policy-input

Qos-policy-input QosInput
        Rate-police 100 50 peak 100 50
        Dscp 32
FTOS#
```

show qos qos-policy-output

View the output QoS policy details.

S5000

Syntax `show qos qos-policy-output [`*`qos-policy-name`*`]`

Parameters

qos-policy-name	Enter the QoS policy name.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show qos qos-policy-output

Qos-policy-output qosOut
        Rate-limit 50 50 peak 50 50
        Wred yellow 1
        Wred green 1
```

show qos statistics

View QoS statistics.

S5000

Syntax `show qos statistics [`*`interface`*`]`

Parameters

interface	Enter one of the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output from the `show qos statistics` command Example below.

Field	Description
Queue #	Queue Number
Queued Bytes	Snapshot of the byte count in that queue.
Matched Pkts	The number of packets that matched the class-map criteria. **NOTE:** When you configure `trust`, matched packet counters are not incremented in this field.
Matched Bytes	The number of bytes that matched the class-map criteria. **NOTE:** When you configure `trust`, matched byte counters are not incremented in this field.

Example (ED, EE)

```
FTOS#show qos statistics

Interface Te 0/0
Queue# Queued Bytes Matched Pkts Matched Bytes
   0     0             0            0
   1     0             0            0
   2     0             0            0
   3     0             0            0
   4     0             0            0
   5     0             0            0
   6     0             0            0
   7     0             0            0

Interface Te 0/1
Queue# Queued Bytes Matched Pkts Matched Bytes
   0     0             0            0
   1     0             0            0
   2     0             0            0
   3     0             0            0
   4     0             0            0
   5     0             0            0
   6     0             0            0
   7     0             0            0
```

Usage Information

The following describes output from the `show qos statistics` command Example below.

Field	Description
Queue #	Queue Number
Queued Bytes (Cumulative)	Snapshot of the byte count in that queue.
Queued Pkts (Cumulative)	Cumulative packet count in that queue.
Matched Pkts	The number of packets that matched the class-map criteria. **NOTE:** When you configure `trust`, matched packet counters are not incremented in this field.
Matched Bytes	The number of bytes that matched the class-map criteria. **NOTE:** When you configure `trust`, matched byte counters are not incremented in this field.
Dropped Pkts	The total of the number of packets dropped for green, yellow and out-of-profile.

Example (EF)

```
FTOS#show qos statistics ten 0/1

Queue# Queued         Queued Matched Matched    Dropped
       Bytes          Pkts   Pkts    Bytes      Pkts
       (Cumulative)  (Cumulative)
  0     0            0       1883725 1883725000 0
  1     0            0       1883725 1883725000 0
  2     0            0       1883725 1883725000 0
  3     0            0       1883725 1883725000 0
  4     0            0       1883725 1883725000 0
  5     0            0       1883724 1883724000 0
  6     0            0       1883720 1883720000 0
  7     0            0       1883720 1883720000 0

FTOS#
```

Related Commands

clear qos statistics – clears counters shown in `show qos statistics`.

show qos wred-profile

View the Weighted Random Early Detection (WRED) profile details.

S5000

Syntax `show qos wred-profile` *`wred-profile-name`*

Parameters

wred-profile-name	Enter the WRED profile name to view the profile details.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show qos wred-profile

Wred-profile-name min-threshold max-threshold
wred_drop         0             0
wred_ge_y         1024          2048
wred_ge_g         2048          4096
wred_teng_y       4096          8192
wred_teng_g       8192          16384
WRED1             2000          7000
```

test cam-usage

Check the Input Policy Map configuration for the CAM usage.

S5000

Syntax `test cam-usage service-policy input` *`policy-map`* `stack—unit {[`*`unit-number`*` port-set `*`portpipe number`*`] | [all]}`

Parameters

service-policy input ***policy-map***	Enter the policy map name.
stack-unit ***unit-number***	(OPTIONAL) Enter the keyword `stack-unit` followed by `all` to get information for all the stack-units or enter the unit number to get information for a specific unit. The range is 0 to 11.
port-set ***portpipe number***	Enter the keywords `port-set` followed by the stack-unit's port pipe number. The range is 0 or 1.

Defaults none

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This features allows you to determine if the CAM has enough space available before applying the configuration on an interface.

An input policy map with both Trust and Class-map configuration, the Class-map rules are ignored and only the Trust rule is programmed in the CAM. In such an instance, the Estimated CAM output column will contain the size of the CAM space required for the Trust rule and not the Class-map rule.

The following describes output from the `text cam-usage service-policy input policy-map stack-unit` command shown in the Example below.

Field	Description
Stack-Unit	Indicates the stack-unit number.
Portpipe	Indicates the portpipe number.
CAM Partition	The CAM space where the rules are added.
Available CAM	Indicates the free CAM space, in the partition, for the classification rules. **NOTE:** The CAM entries reserved for the default rules are not included in the Available CAM column; free entries, from the default rules space, can not be used as a policy map for the classification rules.
Estimated CAM per Port	Indicates the number of free CAM entries required (for the classification rules) to apply the input policy map on a single interface. **NOTE:** The CAM entries for the default rule are not included in this column; a CAM entry for the default rule is always dedicated to a port and is always available for that interface.
Status (Allowed ports)	Indicates if the input policy map configuration on an interface belonging to a stack-unit/port-pipe is successful—Allowed (n)—or not successful— Exception. The allowed number (n) indicates the number of ports in that port-pipe on which the Policy Map can be applied successfully.

NOTE: In a Layer 2 Policy Map, IPv4/IPv6 rules are not allowed; therefore, the output contains only L2ACL CAM partition entries.

Example

```
FTOS# test cam-usage service-policy input pmap_l2 stack-unit
all

For a L2 Input Policy Map pmap_l2, the output must be as
follows,

Stack-| Portpipe| CAM Partn| Avail CAM| Est CAM/Port| Status
unit
------------------------------------------------------------
0       0         L2ACL     500         200           Alwd(2)
0       1         L2ACL     100         200           Excptn
1       0         L2ACL     1000        200           Alwd(5)
1       1         L2ACL     0           200           Excptn
…
…
…
```

```
13      1         L2ACL     400         200             Alwd(2)
FTOS#
```

trust

Specify dynamic classification (DSCP) or dot1p to trust.

S5000

Syntax `trust {diffserv [fallback]| dot1p [fallback]}`

Parameters

diffserv	Enter the keyword `diffserv` to specify trust of DSCP markings.
dot1p	Enter the keyword `dot1p` to specify trust dot1p configuration.
fallback	Enter the keyword `fallback` to classify packets according to their DSCP value as a secondary option in case no match occurs against the configured class maps.

Defaults none

Command Modes CONFIGURATION (conf-policy-map-in)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you configure `trust`, matched bytes/packets counters are not incremented in the `show qos statistics` command.

Dynamic mapping honors packets marked according to the standard definitions of DSCP. The default mapping table is shown below:

Table 11. Default Mapping for DSCP Trust

DSCP/CP hex Range (XXX)	DSCP Definition	Traditional IP Precedence	Internal Queue ID	DSCP/CP Decimal
111XXX		Network Control	3	48–63
110XXX		Internetwork Control	3	48–63
101XXX	EF (Expedited Forwarding)	CRITIC/ECP	2	32–47
100XXX	AF4 (Assured Forwarding)	Flash Override	2	32–47
011XXX	AF3	Flash	1	16–31
010XXX	AF2	Immediate	1	16–31
001XXX	AF1	Priority	0	0–15

DSCP/CP hex Range (XXX)	DSCP Definition	Traditional IP Precedence	Internal Queue ID	DSCP/CP Decimal
000XXX	BE (Best Effort)	Best Effort	0	0–15

wred

Designate the WRED profile to yellow or green traffic.

S5000

Syntax

`wred {yellow | green} profile-name`

To remove the WRED drop precedence, use the no wred {yellow | green} [*profile-name]* command.

Parameters

yellow | green	Enter the keyword `yellow` for yellow traffic. A DSCP value of xxx110 and xxx100 maps to yellow. Enter the keyword green for `green` traffic. A DSCP value of xxx010 maps to green.
profile-name	Enter your WRED profile name in character format (16 character maximum). Or use one of the five pre-defined WRED profile names. Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_.

Defaults

none

Command Modes

CONFIGURATION (conf-qos-policy-out)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use this command to assign drop precedence to green or yellow traffic. If there is no honoring enabled on the input, all the traffic defaults to green drop precedence.

Related Commands

wred-profile – creates a WRED profile and name that profile.

trust – defines the dynamic classification to trust DSCP.

wred-profile

Create a WRED profile and name the profile.

S5000

Syntax

```
wred-profile wred-profile-name
```

To remove an existing WRED profile, use the `no wred-profile` command.

Parameters

wred-profile-name	Enter your WRED profile name in character format (16 character maximum). Or use one of the pre-defined WRED profile names. You can configure up to 26 WRED profiles plus the five pre-defined profiles, for a total of 31 WRED profiles. Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_g.

Defaults

The five pre-defined WRED profiles. When you configure a new profile, the minimum and maximum threshold defaults to predefined wred_ge_g values.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the default pre-defined profiles or configure your own profile. You cannot delete the pre-defined profiles or their default values. This command enables WRED configuration mode—(conf-wred).

Related Commands

threshold – specifies the minimum and maximum threshold values of the WRED profile.

44

Private VLAN (PVLAN)

FTOS supports the private VLAN (PVLAN) feature on the S5000 switch.

Private VLANs extend the FTOS security suite by providing Layer 2 isolation between ports within the same private VLAN. A private VLAN partitions a traditional VLAN into subdomains identified by a primary and secondary VLAN pair. The FTOS private VLAN implementation is based on RFC 3069.

For more information, refer to the following commands.

Private VLAN Concepts

Primary VLAN:

The primary VLAN is the base VLAN and can have multiple secondary VLANs. There are two types of secondary VLAN — community VLAN and isolated VLAN:

- A primary VLAN can have any number of community VLANs and isolated VLANs.
- Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports or trunk ports.

Community VLAN:

A community VLAN is a secondary VLAN of the primary VLAN:

- Ports in a community VLAN can talk to each other. Also, all ports in a community VLAN can talk to all promiscuous ports in the primary VLAN and vice-versa.
- Devices on a community VLAN can communicate with each other using member ports, while devices in an isolated VLAN cannot.

Isolated VLAN:

An isolated VLAN is a secondary VLAN of the primary VLAN:

- Ports in an isolated VLAN cannot talk to each other. Servers would be mostly connected to isolated VLAN ports.
- Isolated ports can talk to promiscuous ports in the primary VLAN, and vice-versa.

Port Types:

- *Community port*: A community port is a port that belongs to a community VLAN and is allowed to communicate with other ports in the same community VLAN and with promiscuous ports.
- *Isolated port*: An isolated port is a port that, in Layer 2, can only communicate with promiscuous ports that are in the same PVLAN.
- *Promiscuous port*: A promiscuous port is a port that is allowed to communicate with any other port type.
- *Trunk port*: A trunk port carries VLAN traffic across switches:
  - A trunk port in a PVLAN is always tagged.
  - Primary or secondary VLAN traffic is carried by the trunk port in Tagged mode. The tag on the packet helps identify the VLAN to which the packet belongs.

- A trunk port can also belong to a regular VLAN (non-private VLAN).

ip local-proxy-arp

Enable/disable Layer 3 communication between secondary VLANs in a private VLAN.

S5000

Syntax

`[no] ip local-proxy-arp`

To disable Layer 3 communication between secondary VLANs in a private VLAN, use the `no ip local-proxy-arp` command in INTERFACE VLAN mode for the primary VLAN.

To disable Layer 3 communication in a particular secondary VLAN, use the `no ip local-proxy-arp` command in INTERFACE VLAN mode for the selected secondary VLAN.

NOTE: Even after you disable `ip-local-proxy-arp` (use `no ip-local-proxy-arp`) in a secondary VLAN, Layer 3 communication may happen between some secondary VLAN hosts, until the address resolution protocol (ARP) timeout happens on those secondary VLAN hosts.

Defaults

Layer 3 communication is disabled between secondary VLANs in a private VLAN.

Command Modes

INTERFACE VLAN

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

private-vlan mode – sets the mode of the selected VLAN to community, isolated, or primary.

private-vlan mapping secondary-vlan – maps secondary VLANs to the selected primary VLAN.

show arp – displays the ARP table.

show interfaces private-vlan – displays the type and status of the PVLAN interfaces.

show vlan private-vlan – displays the PVLANs and/or interfaces that are part of a PVLAN.

switchport mode private-vlan – sets PVLAN mode of the selected port.

private-vlan mode

Set PVLAN mode of the selected VLAN to community, isolated, or primary.

S5000

Syntax

`[no] private-vlan mode {community | isolated | primary}`

To remove the PVLAN configuration, use the `no private-vlan mode {community | isolated | primary}` command syntax.

Parameters

community	Enter the keyword `community` to set the VLAN as a community VLAN.
isolated	Enter the keyword `isolated` to configure the VLAN as an isolated VLAN.
primary	Enter the keyword `primary` to configure the VLAN as a primary VLAN.

Defaults none

Command Modes INTERFACE VLAN

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The VLAN:

- can be in only one mode, either `community`, `isolated`, or `primary`.
- mode ode to `community` or `isolated` even before associating it to a primary VLAN. This secondary VLAN continues to work normally as a normal VLAN even though it is not associated to a primary VLAN. (A syslog message indicates this.)
- must not have a port in it when VLAN mode is being set.

Only ports (and port channels) configured as promiscuous, host, or PVLAN trunk ports (as described above) can be added to the PVLAN. No other regular ports can be added to the PVLAN.

After using this command to configure a VLAN as a primary VLAN, use the `private-vlan mapping secondary-vlan` command to map secondary VLANs to this VLAN.

Related Commands

private-vlan mapping secondary-vlan – maps secondary VLANs to the selected primary VLAN.

show interfaces private-vlan – displays the type and status of the PVLAN interfaces.

show vlan private-vlan – displays the PVLANs and/or interfaces that are part of a PVLAN.

show vlan private-vlan mapping – displays the primary-secondary VLAN mapping.

switchport mode private-vlan – sets PVLAN mode of the selected port.

private-vlan mapping secondary-vlan

Map secondary VLANs to the selected primary VLAN.

S5000

Syntax

```
[no] private-vlan mapping secondary-vlan vlan-list
```

To remove specific secondary VLANs from the configuration, use the `no private-vlan mapping secondary-vlan` *`vlan-list`* command syntax.

Parameters

vlan-list	Enter the list of secondary VLANs to associate with the selected primary VLAN. The list can be in comma-delimited or hyphenated-range format, following the convention for the range input.

Defaults none

Command Modes INTERFACE VLAN

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The list of secondary VLANs can be:

- Specified in comma-delimited or hyphenated-range format.
- Specified with this command even before they have been created.
- Amended by specifying the new secondary VLAN to be added to the list.

Related Commands

private-vlan mode – sets the mode of the selected VLAN to community, isolated, or primary.

show interfaces private-vlan – displays the type and status of the PVLAN interfaces.

show vlan private-vlan – displays the PVLANs and/or interfaces that are part of a PVLAN.

show vlan private-vlan mapping – displays the primary-secondary VLAN mapping.

switchport mode private-vlan – sets PVLAN mode of the selected port.

show interfaces private-vlan

Display type and status of PVLAN interfaces.

S5000

Syntax `show interfaces private-vlan [interface interface]`

Parameters

interface *interface*	(OPTIONAL) Enter the keyword `interface` followed by the ID of the specific interface for which to display PVLAN status.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command has two types of display — a list of all PVLAN interfaces or for a specific interface. Examples of both types of output are shown below.

The following describes output from the `show interfaces private-vlan` command shown in the Examples below.

Field	Description
Interface	Displays the type of interface and associated slot and port number.
Vlan	Displays the VLAN ID of the designated interface.
PVLAN-Type	Displays the type of VLAN in which the designated interface resides.
Interface Type	Displays the PVLAN port type of the designated interface.
Status	States whether the interface is operationally up or down.

Example (All)

```
FTOS# show interfaces private-vlan
Interface Vlan PVLAN-Type Interface Type Status
--------- ---- ---------- -------------- --------
Te 2/1    10   Primary    Promiscuous    Up
Te 2/2    100  Isolated   Host           Down
Te 2/3    10   Primary    Trunk          Up
Te 2/4    101  Community  Host           Up
```

Example (Specific)

```
FTOS# show interfaces private-vlan Te 2/2
Interface Vlan PVLAN-Type Interface Type Status
--------- ---- ---------- -------------- --------
Te 2/2    100  Isolated   Host           Up
```

Related Commands

private-vlan mode – sets the mode of the selected VLAN to community, isolated, or primary.

show vlan private-vlan – displays the PVLANs and/or interfaces that are part of a PVLAN.

show vlan private-vlan mapping – displays the primary-secondary VLAN mapping.

switchport mode private-vlan – sets PVLAN mode of the selected port.

show vlan private-vlan

Display PVLANs and/or interfaces that are part of a PVLAN.

S5000

Syntax

```
show vlan private-vlan [community | interface | isolated |
primary | primary_vlan | interface interface]
```

Parameters

community	(OPTIONAL) Enter the keyword `community` to display VLANs configured as community VLANs, along with their interfaces.
interface	(OPTIONAL) Enter the keyword `interface` to display VLANs configured as community VLANs, along with their interfaces.
isolated	(OPTIONAL) Enter the keyword `isolated` to display VLANs configured as isolated VLANs, along with their interfaces.
primary	(OPTIONAL) Enter the keyword `primary` to display VLANs configured as primary VLANs, along with their interfaces.

primary_vlan	(OPTIONAL) Enter a private VLAN ID or secondary VLAN ID to display interface details about the designated PVLAN.
interface *interface*	(OPTIONAL) Enter the keyword `interface` and an interface ID to display the PVLAN configuration of the designated interface.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Examples of all types of command output are shown below. The first type of output is the result of not entering an optional keyword. It displays a detailed list of all PVLANs and their member VLANs and interfaces. The other types of output show details about PVLAN subsets.

The following describes output from the `show private-vlan` command shown in the Examples below.

Field	Description
Primary	Displays the VLAN ID of the designated or associated primary VLAN(s).
Secondary	Displays the VLAN ID of the designated or associated secondary VLAN(s).
Type	Displays the type of VLAN in which the listed interfaces reside.
Active	States whether the interface is operationally up or down.
Ports	Displays the interface IDs in the listed VLAN.

Example (All)

```
FTOS# show vlan private-vlan
Primary Secondary Type      Active Ports
------- --------- --------- ------ -----------
10                primary   Yes    Te 2/1,3
        100       isolated  Yes    Te 2/2
        101       community Yes    Te 2/10
20                primary   Yes    Po 10, 12-13
                                   Te 3/1
        200       isolated  Yes    Te 3/2,4-6
        201       community No
        202       community Yes    Te 3/11-12
```

Example (Primary)

```
FTOS# show vlan private-vlan primary
Primary Secondary Type    Active  Ports
------- --------- --------- ------ -------
10                primary  Yes    Te 2/1,3
20                primary  Yes    Te 3/1,3
```

Example (Isolated)

```
FTOS# show vlan private-vlan isolated
Primary Secondary Type      Active Ports
------- --------- --------- ------ ----------
10                primary   Yes    Te 2/1,3
```

```
        100       isolated  Yes    Te 2/2,4-6
        200       isolated  Yes    Te 3/2,4-6
```

Example (Community)

```
FTOS# show vlan private-vlan community
Primary Secondary Type      Active Ports
------- --------- --------- ------ -----------
10                primary   Yes    Te 2/1,3
        101       community Yes    Te 2/7-10
20                primary   Yes    Po 10, 12-13
                                   Te 3/1
        201       community No
        202       community Yes    Te 3/11-12
```

Example (Specific)

```
FTOS# show vlan private-vlan interface Te 2/1
Primary Secondary Type     Active Ports
------- --------- --------- --------------------
10                primary  Yes    Te 2/1
```

Usage Information

If the VLAN ID is that of a primary VLAN, the entire private VLAN output is displayed, as shown below. If the VLAN ID is a secondary VLAN, only its primary VLAN and its particular secondary VLAN properties are displayed, as shown in the second Example.

Example

```
FTOS# show vlan private-vlan 10
Primary Secondary Type      Active  Ports
------- --------- --------- -------------------
10                primary   Yes     Te 2/1,3
        102       isolated  Yes     Te 0/4
        101       community Yes     Tei 2/7-10
```

Example

```
FTOS#show vlan private-vlan 102
Primary Secondary Type     Active Ports
------- --------- --------- --------------------
10                Primary  Yes    Po 1
                                  Te 0/2
        102       Isolated Yes    Te 0/4
```

Related Commands

private-vlan mode – sets the mode of the selected VLAN to community, isolated, or primary.

show interfaces private-vlan – displays type and status of PVLAN interfaces.

show vlan private-vlan mapping – displays the primary-secondary VLAN mapping.

switchport mode private-vlan – sets PVLAN mode of the selected port.

show vlan private-vlan mapping

Display primary-secondary VLAN mapping.

S5000

Syntax `show vlan private-vlan mapping`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The output of this command, shown below, displays the community and isolated VLAN IDs that are associated with each primary VLAN.

Example

```
FTOS# show vlan private-vlan mapping
Private Vlan:
  Primary   : 100
  Isolated  : 102
  Community : 101
  Unknown   : 200
```

Related Commands

private-vlan mode – sets the mode of the selected VLAN to community, isolated, or primary.

show interfaces private-vlan – displays type and status of PVLAN interfaces.

show vlan private-vlan mapping – displays the primary-secondary VLAN mapping.

switchport mode private-vlan – sets PVLAN mode of the selected port.

switchport mode private-vlan

Set PVLAN mode of the selected port.

S5000

Syntax

`[no] switchport mode private-vlan {host | promiscuous | trunk}`

To remove PVLAN mode from the selected port, use the `no switchport mode private-vlan` command.

Parameters

host	Enter the keyword `host` to configure the selected port or port channel as an isolated interface in a PVLAN.
promiscuous	Enter the keyword `promiscuous` to configure the selected port or port channel as an promiscuous interface.
trunk	Enter the keyword `trunk` to configure the selected port or port channel as a trunk port in a PVLAN.

Defaults Disabled.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The assignment of the various PVLAN port types to port and port channel (LAG) interfaces is shown below.

Example

```
FTOS#conf
FTOS(conf)#interface TenGigabitEthernet 2/1
FTOS(conf-if-te-2/1)#switchport mode private-vlan promiscuous

FTOS(conf)#interface TenGigabitEthernet 2/2
FTOS(conf-if-te-2/2)#switchport mode private-vlan host

FTOS(conf)#interface TenGigabitEthernet 2/3
FTOS(conf-if-te-2/3)#switchport mode private-vlan trunk

FTOS(conf)#interface port-channel 10
FTOS(conf-if-te-2/3)#switchport mode private-vlan promiscuous
```

Related Commands

private-vlan mode – sets the mode of the selected VLAN to community, isolated, or primary.

private-vlan mapping secondary-vlan – sets the mode of the selected VLAN to primary and then associates the secondary VLANs to it.

show interfaces private-vlan – displays type and status of PVLAN interfaces.

show vlan private-vlan mapping – displays the primary-secondary VLAN mapping.

45

Routing Information Protocol (RIP)

Routing information protocol (RIP) is a distance vector routing protocol. The Dell Networking operating software (FTOS) supports both RIP version 1 (RIPv1) and RIP version 2 (RIPv2) on the S5000.

NOTE: For more information about configuring RIP, refer to the *FTOS Configuration Guide*.

auto-summary

Restore the default behavior of automatic summarization of subnet routes into network routes. This command applies only to RIP version 2.

S5000

Syntax `auto-summary`

To send sub-prefix routing information, use the `no auto-summary` command.

Defaults Enabled.

Command Modes ROUTER RIP

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear ip rip

Update all the RIP routes in the FTOS routing table.

S5000

Syntax `clear ip rip`

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This command triggers updates of the main RIP routing tables.

debug ip rip

Examine RIP routing information for troubleshooting.

S5000

Syntax

```
debug ip rip [database | [events [interface-type slot/port] |
packet [interface-type slot/port]] | trigger]
```

To turn off debugging output, use the `no debug ip rip` command.

Parameters

interface-type slot/port	(OPTIONAL) Enter the interface type and ID as one of the following: - For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. - For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. - For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094. **NOTE:** This option is available on the S5000 as a sub-option.
database	(OPTIONAL) Enter the keyword `database` to display messages when there is a change to the RIP database.
events	(OPTIONAL) Enter the keyword `events` to debug only RIP protocol changes.
trigger	(OPTIONAL) Enter the keyword `trigger` to debug only RIP trigger extensions.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

default-information originate

Generate a default route for the RIP traffic.

S5000

Syntax

```
default-information originate [always] [metric metric-value]
[route-map map-name]
```

To return to the default values, use the `no default-information originate` command.

Parameters

always	(OPTIONAL) Enter the keyword `always` to enable the switch software to always advertise the default route.
metric ***metric-value***	(OPTIONAL) Enter the keyword `metric` followed by a number as the metric value. The range is 1 to 16. The default is 1.
route-map ***map-name***	(OPTIONAL) Enter the keywords `route-map` followed by the name of a configured route-map.

Defaults Disabled. Metric: 1.

Command Modes ROUTER RIP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The default route must be present in the switch routing table for the `default-information originate` command to take effect.

default-metric

Change the default metric for routes. Use this command with the `redistribute` command to ensure that all redistributed routes use the same metric value.

S5000

Syntax `default-metric` *`number`*

To return the default metric to the original values, use the `no default-metric` command.

Parameters

number	Specify a number. The range is 1 to 16. The default is 1.

Defaults 1

Command Modes ROUTER RIP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This command ensures that route information being redistributed is converted to the same metric value.

Related Commands redistribute – allows you to redistribute routes learned by other methods.

description

Enter a description of the RIP routing protocol.

S5000

Syntax

`description {description}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description to identify the RIP protocol (80 characters maximum).

Defaults

none

Command Modes

ROUTER RIP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

router rip – enters ROUTER mode on the switch.

distance

Assign a weight (for prioritization) to all routes in the RIP routing table or to a specific route. Lower weights (“administrative distance”) are preferred.

S5000

Syntax

`distance weight [ip-address mask [prefix-name]]`

To return to the default values, use the `no distance weight [ip-address mask]` command.

Parameters

weight	Enter a number from 1 to 255 for the weight (for prioritization). The default is **120**.
ip-address	(OPTIONAL) Enter the IP address, in dotted decimal format (A.B.C.D), of the host or network to receive the new distance metric.
mask	If you enter an IP address, you must also enter a mask for that IP address, in either dotted decimal format or /prefix format (/x).
prefix-name	(OPTIONAL) Enter a configured prefix list name.

Defaults

weight = **120**

Command Modes

ROUTER RIP

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Related Commands

default-metric – assigns one distance metric to all routes learned using the `redistribute` command.

distribute-list in

Configure a filter for incoming routing updates.

S5000

Syntax

`distribute-list prefix-list-name in [interface-type slot/port]`

To delete the filter, use the `no distribute-list prefix-list-name in` command.

Parameters

***prefix-list-name* in**	Enter the name of a configured prefix list followed by the keyword `in`.
interface-type slot/port	(OPTIONAL) Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults

Not configured.

Command Modes

ROUTER RIP

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Related Commands

ip prefix-list – enters PREFIX-LIST mode and configures a prefix list.

distribute-list out

Configure a filter for outgoing routing updates.

S5000

Syntax

`distribute-list prefix-list-name out [interface-type slot/port | bgp | connected | ospf | static]`

To delete the filter, use the `no distribute-list prefix-list-name out` command.

Parameters

***prefix-list-name* out**	Enter the name of a configured prefix list followed by the keyword `out`.
interface-type slot/port	(OPTIONAL) Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
connected	(OPTIONAL) Enter the keyword `connected` to filter only directly connected routes.
ospf	(OPTIONAL) Enter the keyword `ospf` to filter all OSPF routes.
static	(OPTIONAL) Enter the keyword `static` to filter manually configured routes.

Defaults

Not configured.

Command Modes

ROUTER RIP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

ip prefix-list – enters PREFIX-LIST mode and configures a prefix list.

ip poison-reverse

Set the prefix of the RIP routing updates to the RIP infinity value.

S5000

Syntax	`ip poison-reverse` To disable poison reverse, use the `no ip poison-reverse` command.
Defaults	Disabled.
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	ip split-horizon – sets the RIP routing updates to exclude routing prefixes.

ip rip receive version

Set the interface to receive specific versions of RIP. The RIP version you set on the interface overrides the version command in ROUTER RIP mode.

S5000

Syntax	`ip rip receive version [1] [2]` To return to the default, use the `no ip rip receive version` command.
Parameters	**1** (OPTIONAL) Enter the number `1` for RIP version 1. **2** (OPTIONAL) Enter the number `2` for RIP version 2.
Defaults	RIPv1 and RIPv2
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	If you want the interface to receive both versions of RIP, use the `ip rip receive version 1 2` command.
Related Commands	ip rip send version – sets the RIP version to be used for sending RIP traffic on an interface. version – sets the RIP version to be used for the switch software.

ip rip send version

Set the interface to send a specific version of RIP. The version you set on the interface overrides the version command in ROUTER RIP mode.

S5000

Syntax	`ip rip send version [1] [2]` To return to the default value, use the `no ip rip send version` command.
Parameters	**1** — (OPTIONAL) Enter the number `1` for RIP version 1. The default is RIPv1. **2** — (OPTIONAL) Enter the number `2` for RIP version 2.
Defaults	RIPv1
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** — Introduced on the S5000.
Usage Information	To enable the interface to send both version of RIP packets, use the `ip rip send version 1 2` command.
Related Commands	ip rip receive version – sets the RIP version for the interface to receive traffic. version – sets the RIP version to be used for the switch software.

ip split-horizon

Enable split-horizon for RIP data on the interface. As described in RFC 2453, the split-horizon scheme prevents any routes learned over a specific interface to be sent back out that interface.

S5000

Syntax	`ip split-horizon` To disable split-horizon, use the `no ip split-horizon` command.
Defaults	Enabled
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** — Introduced on the S5000.
Related Commands	ip poison-reverse – sets the prefix for RIP routing updates.

maximum-paths

Set RIP to forward packets over multiple paths.

S5000

Syntax

`maximum-paths number`

To return to the default values, use the `no maximum-paths` commands.

Parameters

number	Enter the number of paths. The range is 1 to 16. The default is **4** paths.

Defaults

4

Command Modes

ROUTER RIP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

RIP supports a maximum of 16 ECMP paths.

neighbor

Define a neighbor router with which to exchange RIP information.

S5000

Syntax

`neighbor ip-address`

To delete a neighbor setting, use the `no neighbor ip-address` command.

Parameters

ip-address	Enter the IP address, in dotted decimal format, of a router with which to exchange information.

Defaults

Not configured.

Command Modes

ROUTER RIP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When a neighbor router is identified, unicast data exchanges occur. Multiple neighbor routers are possible.

Use the `passive-interface` command in conjunction with the `neighbor` command to ensure that only specific interfaces are receiving and sending data.

Related Commands

passive-interface – sets the interface to only listen to RIP broadcasts.

network

Enable RIP for a specified network. Use this command to enable RIP on all networks connected to the switch.

S5000

Syntax

`network ip-address`

To disable RIP for a network, use the `no network ip-address` command.

Parameters

ip-address	Specify an IP network address in dotted decimal format. You cannot specify a subnet.

Defaults

No RIP network is configured.

Command Modes

ROUTER RIP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can enable an unlimited number of RIP networks.

RIP operates over interfaces configured with any address specified by the `network` command.

offset-list

Specify a number to add to the incoming or outgoing route metrics learned using RIP.

S5000

Syntax

`offset-list prefix-list-name {in | out} offset [interface-type slot/port]`

To delete an offset list, use the `no offset-list prefix-list-name {in | out} offset [interface-type slot/port]` command.

Parameters

prefix-list-name	Enter the name of an established Prefix list to determine which incoming routes will be modified.
offset	Enter a number from zero (0) to 16 to be applied to the incoming route metric matching the access list specified. If you set an offset value to zero (0), no action is taken.
interface-type slot/port	(OPTIONAL) Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults Not configured.

Command Modes ROUTER RIP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information When the offset metric is applied to an interface, that value takes precedence over an offset value that is not extended to an interface.

Related Commands ip prefix-list – enters PREFIX-LIST mode and configure a prefix list.

output-delay

Set the interpacket delay of successive packets to the same neighbor.

S5000

Syntax `output-delay` *`delay`*

To return to the switch software defaults for interpacket delay, use the `no output-delay` command.

Parameters

delay	Specify a number of milliseconds as the delay interval. The range is 8 to 50.

Defaults Not configured.

Command Modes ROUTER RIP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This command is intended for low-speed interfaces.

passive-interface

Suppress routing updates on a specified interface.

S5000

Syntax	`passive-interface` *`interface-type slot/port`* To delete a passive interface, use the `no passive-interface` *`interface-type slot/port`* command.
Parameters	*interface-type slot/port*: Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
Defaults	Not configured.
Command Modes	ROUTER RIP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Although the passive interface does not send or receive routing updates, the network on that interface is still included in RIP updates sent through other interfaces.
Related Commands	neighbor – defines a neighbor. network – enables RIP for a specified network.

redistribute

Redistribute information from other routing instances.

S5000

Syntax	`redistribute {connected	static}` To disable redistribution, use the no redistribute {connected | static} command.

Parameters

connected	Enter the keyword `connected` to specify that information from active routes on interfaces is redistributed.
static	Enter the keyword `static` to specify that information from static routes is redistributed.

Defaults Not configured.

Command Modes ROUTER RIP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information To redistribute the default route (0.0.0.0/0), configure the `default-information originate` command.

Related Commands default-information originate – generates a default route for RIP traffic.

redistribute isis

Redistribute routing information from an IS-IS instance.

S5000

Syntax `redistribute isis [`*`tag`*`] [level-1 | level-1-2 | level-2] [metric `*`metric-value`*`] [route-map `*`map-name`*`]`

To disable redistribution, use the `no redistribute isis [`*`tag`*`] [level-1 | level-1-2 | level-2] [metric `*`metric-value`*`] [route-map `*`map-name`*`]` command.

Parameters

tag	(OPTIONAL) Enter the name of the IS-IS routing process.
level-1	(OPTIONAL) Enter the keywords `level-1` to redistribute only IS-IS Level-1 routes.
level-1-2	(OPTIONAL) Enter the keywords `level-1-2` to redistribute both IS-IS Level-1 and Level-2 routes.
level-2	(OPTIONAL) Enter the keywords `level-2` to redistribute only IS-IS Level-2 routes.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` followed by a number as the metric value. The range is 0 to 16.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of a configured route map.

Defaults Not configured.

Command Modes	ROUTER RIP
Command History	**Version 9.0(1.3)** Introduced on the S5000.

redistribute ospf

Redistribute routing information from an OSPF process.

S5000

Syntax

`redistribute ospf` *`process-id`* `[match external {1 | 2} | match internal | metric` *`metric-value`*`] [route-map` *`map-name`*`]`

To disable redistribution, use the `no redistribute ospf` *`process-id`* `[match external {1 | 2} | match internal | metric` *`metric-value`*`] [route-map` *`map-name`*`]` command.

Parameters

process-id	Enter a number that corresponds to the OSPF process ID to be redistributed. The range is 1 to 65355.
match external {1 | 2}	(OPTIONAL) Enter the keywords `match external` followed by the numbers `1` or `2` to indicated that external 1 routes or external 2 routes should be redistributed.
match internal	(OPTIONAL) Enter the keywords `match internal` to indicate that internal routes should be redistributed.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` followed by a number as the metric value. The range is 0 to 16.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of a configured route map.

Defaults	Not configured.
Command Modes	ROUTER RIP
Command History	**Version 9.0(1.3)** Introduced on the S5000.

router rip

Enter ROUTER RIP mode to configure and enable RIP.

S5000

Syntax

`router rip`

To disable RIP, use the `no router rip` command.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To enable RIP, you must assign a network address using the `network` command.

Example

```
FTOS(conf)#router rip
FTOS(conf-router_rip)#
```

Related Commands

network – enables RIP.

exit – returns to CONFIGURATION mode.

show config

Display the changes you made to the RIP configuration. Default values are not shown.

S5000

Syntax

`show config`

Command Modes

ROUTER RIP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-router_rip)#show config
!
router rip
  network 172.31.0.0
  passive-interface TenGigabitEthernet 0/1
FTOS(conf-router_rip)#
```

show ip rip database

Display the routes that RIP learns. If the switch learned no RIP routes, no output is generated.

S5000

Syntax `show ip rip database [ip-address mask]`

Parameters

ip-address	(OPTIONAL) Specify an IP address in dotted decimal format to view RIP information on that network only. If you enter an IP address, you must also enter a mask for that IP address.
mask	(OPTIONAL) Specify a mask, in /network format, for the IP address.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The following describes the `show ip rip database` command shown in the Example below.

Field	Description
Total number of routes in RIP database	Displays the number of RIP routes stored in the RIP database.
100.10.10.0/24 directly connected	Lists the route(s) directly connected.
150.100.0.0 redistributed	Lists the routes learned through redistribution.
209.9.16.0/24...	Lists the routes and the sources advertising those routes.

Example

```
FTOS#show ip rip database
Total number of routes in RIP database: 1624
204.250.54.0/24
      [50/1] via 192.14.1.3, 00:00:12, TenGigabitEthernet 9/15
204.250.54.0/24     auto-summary
203.250.49.0/24
      [50/1] via 192.13.1.3, 00:00:12, TenGigabitEthernet 9/14
203.250.49.0/24     auto-summary
210.250.40.0/24
      [50/2] via 1.1.18.2, 00:00:14, Vlan 18
      [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
210.250.40.0/24     auto-summary
207.250.53.0/24
      [50/2] via 1.1.120.2, 00:00:55, Port-channel 20
      [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
      [50/2] via 1.1.10.2, 00:00:18, Vlan 10
207.250.53.0/24     auto-summary
208.250.42.0/24
      [50/2] via 1.1.120.2, 00:00:55, Port-channel 20
      [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
      [50/2] via 1.1.10.2, 00:00:18, Vlan 10
208.250.42.0/24     auto-summary
```

show running-config rip

Display the current RIP configuration.

S5000

Syntax

```
show running-config rip
```

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
show running-config rip
!
router rip
  distribute-list Test1 in
  distribute-list Test21 out
  network 10.0.0.0
  passive-interface TenGigabitEthernet 2/0
  neighbor 20.20.20.20
  redistribute ospf 999
  version 2
```

timers basic

Manipulate the RIP timers for routing updates, invalid, holddown times, and flush time.

S5000

Syntax `timers basic update` *`invalid holddown flush`*

To return to the default settings, use the `no timers basic` command.

Parameters

update	Enter the number of seconds to specify the rate at which RIP routing updates are sent. The range is zero (0) to 4294967295. The default is **30 seconds**.
invalid	Enter the number of seconds to specify the time interval before routing updates are declared invalid or expired. The invalid value should be at least three times the update timer value. The range is zero (0) to 4294967295. The default is **180 seconds**.

holddown	Enter the number of seconds to specify a time interval during which the route is marked as unreachable but still sending RIP packets. The holddown value should be at least three times the update timer value. The range is zero (0) to 4294967295. The default is **180 seconds**.
flush	Enter the number of seconds to specify the time interval during which the route is advertised as unreachable. When this interval expires, the route is flushed from the routing table. The flush value should be greater than the update value. The range is zero (0) to 4294967295. The default is **240 seconds**.

Defaults

- update = **30 seconds**
- invalid = **180 seconds**
- holddown = **180 seconds**
- flush = **240 seconds**

Command Modes ROUTER RIP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If you change the timers on one router, the timers on all routers in the RIP domain must also be synchronized.

version

Specify either RIP version 1 or RIP version 2.

S5000

Syntax `version {1 | 2}`

To return to the default version setting, use the `no version` command.

Parameters

1	Enter the keyword `1` to specify RIP version 1.
2	Enter the keyword `2` to specify RIP version 2.

Defaults The FTOS sends RIPv1 and receives RIPv1 and RIPv2.

Command Modes ROUTER RIP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

ip rip receive version – sets the RIP version to be received on the interface.

ip rip send version – sets the RIP version to be sent out the interface.

46

Remote Monitoring (RMON)

FTOS supports remote monitoring (RMON) on the S5000 switch.

FTOS RMON is based on IEEE standards, providing both 32-bit and 64-bit monitoring and long-term statistics collection. FTOS RMON supports the following RMON groups, as defined in RFC-2819, RFC-3273, and RFC-3434:

- Ethernet Statistics Table; RFC-2819
- Ethernet Statistics High-Capacity Table; RFC-3273, 64bits
- Ethernet History Control Table; RFC-2819
- Ethernet History Table; RFC-2819
- Ethernet History High-Capacity Table; RFC-3273, 64bits
- Alarm Table; RFC-2819
- High-Capacity Alarm Table (64bits); RFC-3434, 64bits
- Event Table; RFC-2819
- Log Table; RFC-2819

FTOS RMON does not support the following statistics:

- etherStatsCollisions
- etherHistoryCollisions
- etherHistoryUtilization

NOTE: Only SNMP GET/GETNEXT access is supported. Configure RMON using the RMON commands. Collected data is lost during a chassis reboot.

rmon alarm

Set an alarm on any MIB object.

S5000

Syntax

```
rmon alarm number variable interval {delta | absolute} rising-threshold value event-number falling-threshold value event-number [owner string]
```

To disable the alarm, use the `no rmon alarm number` command.

Parameters

number	Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON alarm table.
variable	Enter the MIB object to monitor. The variable must be in the SNMP OID format; for example, 1.3.6.1.2.1.1.3. The object type must be a 32 bit integer.

interval	Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON alarm table. The range is 5 to 3600 seconds.
delta	Enter the keyword `delta` to test the change between MIB variables. This is the alarmSampleType in the RMON alarm table.
absolute	Enter the keyword `absolute` to test each MIB variable directly. This is the alarmSampleType in the RMON alarm table.
rising-threshold *value event-number*	Enter the keywords `rising-threshold` followed by the value (32 bit) the rising-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the rising threshold exceeds its limit. This value is the same as the alarmRisingEventIndex or alarmTable of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.
falling-threshold *value event-number*	Enter the keywords `falling-threshold` followed by the value (32 bit) the falling-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the falling threshold exceeds its limit. This value is the same as the alarmFallingEventIndex or the alarmTable of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.
owner *string*	(OPTIONAL) Enter the keyword `owner` followed by the owner name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB.

Defaults owner

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

rmon collection history

Enable the RMON MIB history group of statistics collection on an interface.

S5000

Syntax

```
rmon collection history {controlEntry integer} [owner name]
[buckets number] [interval seconds]
```

To remove a specified RMON history group of statistics collection, use the `no rmon collection history {controlEntry integer}` command.

Parameters

controlEntry *integer*	Enter the keyword `controlEntry` to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON group of statistics. The integer value must be a unique index in the RMON history table.

owner *name*	(OPTIONAL) Enter the keyword `owner` followed by the owner name to record the owner of the RMON group of statistics.
buckets *number*	(OPTIONAL) Enter the keyword `buckets` followed the number of buckets for the RMON collection history group of statistics. The bucket range is 1 to 1000. The default is **50**.
interval *seconds*	(OPTIONAL) Enter the keyword `interval` followed the number of seconds in each polling cycle. The range is 5 to 3600 seconds. The default is **1800 seconds**.

Defaults none

Command Modes CONFIGURATION INTERFACE (config-if)

Command History

Version 9.0(1.3)	Introduced on the S5000.

rmon collection statistics

Enable RMON MIB statistics collection on an interface.

S5000

Syntax

```
rmon collection statistics {controlEntry integer} [owner name]
```

To remove RMON MIB statistics collection on an interface, use the `no rmon collection statistics {controlEntry integer}` command.

Parameters

controlEntry *integer*	Enter the keyword `controlEntry` to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON Statistic Table. The integer value must be a unique in the RMON statistic table.
owner *name*	(OPTIONAL) Enter the keyword `owner` followed by the owner name to record the owner of the RMON group of statistics.

Defaults none

Command Modes CONFIGURATION INTERFACE (config-if)

Command History

Version 9.0(1.3)	Introduced on the S5000.

rmon event

Add an event in the RMON event table.

S5000

Syntax

```
rmon event number [log] [trap community] [description string]
[owner name]
```

To disable RMON on an interface, use the `no rmon event number [log] [trap community] [description string]` command.

Parameters

number	Assign an event number in integer format from 1 to 65535. The number value must be unique in the RMON event table.
log	(OPTIONAL) Enter the keyword `log` to generate an RMON log entry. The log entry is triggered and sets the eventType in the RMON MIB to log or log-and-trap. The default is **No log**.
trap *community*	(OPTIONAL) Enter the keyword `trap` followed by an SNMP community string to configure the eventType setting in the RMON MIB. This sets either snmp-trap or log-and-trap. The default is **public**.
description *string*	(OPTIONAL) Enter the keyword `description` followed by a string describing the event.
owner *name*	(OPTIONAL) Enter the keyword `owner` followed by the name of the owner of this event.

Defaults As noted above.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

rmon hc-alarm

Set an alarm on any MIB object.

S5000

Syntax

```
rmon hc-alarm number variable interval {delta | absolute}
rising-threshold value event-number falling-threshold value
event-number [owner string]
```

To disable the alarm, use the `no rmon hc-alarm number` command.

Parameters

number	Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON alarm table.

variable	The MIB object to monitor. The variable must be in the SNMP OID format; for example, 1.3.6.1.2.1.1.3 The object type must be a 64 bit integer.
interval	Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON alarm table. The range is 5 to 3600 seconds.
delta	Enter the keyword `delta` to test the change between MIB variables. This is the alarmSampleType in the RMON alarm table.
absolute	Enter the keyword `absolute` to test each MIB variable directly. This is the alarmSampleType in the RMON alarm table.
rising-threshold *value event-number*	Enter the keywords `rising-threshold` followed by the value (64 bit) the rising-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the rising threshold exceeds its limit. This value is the same as the alarmRisingEventIndex or alarmTable of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.
falling-threshold *value event-number*	Enter the keywords `falling-threshold` followed by the value (64 bit) the falling-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the falling threshold exceeds its limit. This value is the same as the alarmFallingEventIndex or the alarmTable of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.
owner *string*	(OPTIONAL) Enter the keyword `owner` followed the owner name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB.

Defaults owner

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

show rmon

Display the RMON running status including the memory usage.

S5000

Syntax `show rmon`

Defaults none

Command Modes EXEC

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Example

```
FTOS# show rmon
RMON status
  total memory used 218840 bytes.
  ether statistics table: 8 entries, 4608 bytes
  ether history table: 8 entries, 6000 bytes
  alarm table: 390 entries, 102960 bytes
  high-capacity alarm table: 5 entries, 1680 bytes
  event table: 500 entries, 206000 bytes
  log table: 2 entries, 552 bytes
FTOS#
```

show rmon alarms

Display the contents of the RMON alarm table.

S5000

Syntax `show rmon alarms [index] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON alarm table in an easy-to-read format.

Defaults none

Command Modes EXEC

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Example (Index)

```
FTOS#show rmon alarm 1
RMON alarm entry 1
  sample Interval: 5
  object: 1.3.6.1.2.1.1.3
  sample type: absolute value.
  value: 255161
  alarm type: rising or falling alarm.
  rising threshold: 1, RMON event index: 1
  falling threshold: 501, RMON event index: 501
  alarm owner: 1
  alarm status: OK
FTOS#
```

Example (Brief)

```
FTOS#show rmon alarm br
index   SNMP OID
--------------------------
1       1.3.6.1.2.1.1.3
2       1.3.6.1.2.1.1.3
3       1.3.6.1.2.1.1.3
4       1.3.6.1.2.1.1.3
```

```
5       1.3.6.1.2.1.1.3
6       1.3.6.1.2.1.1.3
7       1.3.6.1.2.1.1.3
8       1.3.6.1.2.1.1.3
9       1.3.6.1.2.1.1.3
10      1.3.6.1.2.1.1.3
11      1.3.6.1.2.1.1.3
12      1.3.6.1.2.1.1.3
13      1.3.6.1.2.1.1.3
14      1.3.6.1.2.1.1.3
15      1.3.6.1.2.1.1.3
16      1.3.6.1.2.1.1.3
17      1.3.6.1.2.1.1.3
18      1.3.6.1.2.1.1.3
19      1.3.6.1.2.1.1.3
20      1.3.6.1.2.1.1.3
21      1.3.6.1.2.1.1.3
22      1.3.6.1.2.1.1.3
FTOS#
```

show rmon events

Display the contents of the RMON event table.

S5000

Syntax `show rmon events [index] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON event table in an easy-to-read format.

Defaults none

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (Index)

```
FTOS#show rmon event 1
RMON event entry 1
  description: 1
  event type: LOG and SNMP TRAP.
  event community: public
  event last time sent: none
  event owner: 1
  event status: OK
FTOS#
```

Example (Brief)

```
FTOS#show rmon event br
index    description
------------------------------
1        1
2        2
```

```
3        3
4        4
5        5
6        6
7        7
8        8
9        9
10       10
11       11
12       12
13       13
14       14
15       15
16       16
17       17
18       18
19       19
20       20
21       21
22       22
FTOS#
```

show rmon hc-alarm

Display the contents of RMON High-Capacity alarm table.

S5000

Syntax

```
show rmon hc-alarm [index] [brief]
```

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON High-Capacity alarm table in an easy-to-read format.

Defaults none

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (Index)

```
FTOS#show rmon hc-alarm 1
RMON high-capacity alarm entry 1
  object: 1.3.6.1.2.1.1.3
  sample interval: 5
  sample type: absolute value.
  value: 185638
  alarm type: rising or falling alarm.
  alarm rising threshold value: positive.
  rising threshold: 1001, RMON event index: 1
  alarm falling threshold value: positive.
  falling threshold: 999, RMON event index: 6
  alarm sampling failed 0 times.
  alarm owner: 1
  alarm storage type: non-volatile.
  alarm status: OK
FTOS#
```

Example (Brief)

```
FTOS#show rmon hc-alarm brief
index     SNMP OID
----------------------------------
1         1.3.6.1.2.1.1.3
2         1.3.6.1.2.1.1.3
3         1.3.6.1.2.1.1.3
4         1.3.6.1.2.1.1.3
5         1.3.6.1.2.1.1.3
FTOS#
```

show rmon history

Display the contents of the RMON Ethernet history table.

S5000

Syntax `show rmon history [index] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON Ethernet history table in an easy-to-read format

Defaults none

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (Index)

```
FTOS#show rmon history 6001
RMON history control entry 6001
  interface: ifIndex.100974631 TenGigabitEthernet 2/0
  bucket requested: 1
  bucket granted: 1
  sampling interval: 5 sec
  owner: 1
  status: OK
FTOS#
```

Example (Brief)

```
FTOS#show rmon history brief
index    ifIndex      interface
---------------------------------------
6001    100974631    TenGigabitEthernet 2/0
6002    100974631    TenGigabitEthernet 2/0
6003    101236775    TenGigabitEthernet 2/1
6004    101236775    TenGigabitEthernet 2/1
9001    134529054    TenGigabitEthernet 3/0
9002    134529054    TenGigabitEthernet 3/0
9003    134791198    TenGigabitEthernet 3/1
```

```
9004    134791198    TenGigabitEthernet 3/1
FTOS#
```

show rmon log

Display the contents of the RMON log table.

S5000

Syntax `show rmon log [index] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON log table in an easy-to-read format.

Defaults none

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The log table has a maximum of 500 entries. If the log exceeds that maximum, the oldest log entry is purged to allow room for the new entry.

Example (Index)

```
FTOS#show rmon log 2
RMON log entry, alarm table index 2, log index 1
  log time: 14638 (THU AUG 12 22:10:40 2004)
  description: 2
FTOS#
```

Example (Brief)

```
FTOS#show rmon log br
eventIndex     description
------------------------------
2              2
4              4
FTOS#
```

show rmon statistics

Display the contents of RMON Ethernet statistics table.

S5000

Syntax `show rmon statistics [index] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON Ethernet statistics table in an easy-to-read format.

Defaults none

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (Index)

```
FTOS#show rmon statistics 6001
RMON statistics entry 6001
  interface: ifIndex.100974631 TenGigabitEthernet 2/0
  packets dropped: 0
  bytes received: 0
  packets received: 0
  broadcast packets: 0
  multicast packets: 0
  CRC error: 0
  under-size packets: 0
  over-size packets: 0
  fragment errors: 0
  jabber errors: 0
  collision: 0
  64bytes packets: 0
  65-127 bytes packets: 0
  128-255 bytes packets: 0
  256-511 bytes packets: 0
  512-1023 bytes packets: 0
  1024-1518 bytes packets: 0
  owner: 1
  status: OK
  <high-capacity data>
  HC packets received overflow: 0
  HC packets received: 0
  HC bytes received overflow: 0
  HC bytes received: 0
  HC 64bytes packets overflow: 0
  HC 64bytes packets: 0
  HC 65-127 bytes packets overflow: 0
  HC 65-127 bytes packets: 0
  HC 128-255 bytes packets overflow: 0
  HC 128-255 bytes packets: 0
  HC 256-511 bytes packets overflow: 0
  HC 256-511 bytes packets: 0
  HC 512-1023 bytes packets overflow: 0
  HC 512-1023 bytes packets: 0
  HC 1024-1518 bytes packets overflow: 0
  HC 1024-1518 bytes packets: 0
FTOS#
```

Example (Brief)

```
FTOS#show rmon statistics br
index    ifIndex    interface
----------------------------------------
6001    100974631    TenGigabitEthernet 2/0
6002    100974631    TenGigabitEthernet 2/0
6003    101236775    TenGigabitEthernet 2/1
6004    101236775    TenGigabitEthernet 2/1
9001    134529054    TenGigabitEthernet 3/0
```

```
9002    134529054    TenGigabitEthernet 3/0
9003    134791198    TenGigabitEthernet 3/1
9004    134791198    TenGigabitEthernet 3/1
FTOS#
```

47

Rapid Spanning Tree Protocol (RSTP)

The Dell Networking operating software (FTOS) implementation of rapid spanning tree protocol (RSTP) is based on the IEEE 802.1w standard spanning-tree protocol. The RSTP algorithm configures connectivity throughout a bridged local area network (LAN) that is comprised of LANs interconnected by bridges.

FTOS supports RSTP on the S5000.

bridge-priority

Set the bridge priority for RSTP.

S5000

Syntax

`bridge-priority priority-value`

To return to the default value, use the `no bridge-priority` command.

Parameters

priority-value	Enter a number as the bridge priority value in increments of 4096. The range is 0 to 61440. The default is **32768**.

Defaults **32768**

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands protocol spanning-tree rstp – enters rapid spanning tree mode.

debug spanning-tree rstp

Enable debugging of RSTP and view information on the protocol.

S5000

Syntax

```
debug spanning-tree rstp [all | bpdu interface-type slot/port
{in | out} | events]
```

To disable debugging, use the `no debug spanning-tree rstp` command.

Parameters

all	(OPTIONAL) Enter the keyword `all` to debug all spanning tree operations.
bpdu *interface-type slot/port* {in | out}	(OPTIONAL) Enter the keyword `bpdu` to debug the bridge protocol data units. (OPTIONAL) Enter the keyword `interface` along with the type slot/port of the interface you want displayed. Type slot/port options are the following: - For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. - For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. Optionally, enter an in or out parameter in conjunction with the optional interface: - For Receive, enter `in`. - For Transmit, enter `out`.
events	(OPTIONAL) Enter the keyword `events` to debug RSTP events.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#debug spanning-tree rstp bpdu tengigabitethernet 2/0 ?
in Receive (in)
out Transmit (out)
```

description

Enter a description of the rapid spanning tree.

S5000

Syntax `description {description}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description to identify the rapid spanning tree (80 characters maximum).

Defaults	none
Command Modes	SPANNING TREE (The prompt is “config-rstp”.)
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	protocol spanning-tree rstp – enters SPANNING TREE mode on the switch.

disable

Disable RSTP globally on the system.

S5000

Syntax	`disable` To enable Rapid Spanning Tree Protocol, use the `no disable` command.
Defaults	RSTP is disabled.
Command Modes	CONFIGURATION RSTP (conf-rstp)
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	protocol spanning-tree rstp – enters SPANNING TREE mode on the switch.

forward-delay

Configure the amount of time the interface waits in the Listening State and the Learning State before transitioning to the Forwarding State.

S5000

Syntax	`forward-delay` *`seconds`* To return to the default setting, use the `no forward-delay` command.
Parameters	***seconds*** Enter the number of seconds that FTOS waits before transitioning RSTP to the forwarding state. The range is 4 to 30. The default is 15 seconds.
Defaults	15 seconds
Command Modes	CONFIGURATION RSTP (conf-rstp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

hello-time – changes the time interval between BPDUs.

max-age – changes the wait time before RSTP refreshes the protocol configuration information.

hello-time

Set the time interval between the generation of the RSTP bridge protocol data units (BPDUs).

S5000

Syntax

`hello-time [milli-second] seconds`

To return to the default value, use the `no hello-time` command.

Parameters

seconds	Enter a number as the time interval between transmission of BPDUs. The range is 1 to 10 seconds. The default is **2 seconds**.
milli-second	Enter the keywords `milli-second` to configure a hello time on the order of milliseconds. The range is 50 to 950 milliseconds

Defaults

2 seconds

Command Modes

CONFIGURATION RSTP (conf-rstp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The hello time is encoded in BPDUs in increments of 1/256ths of a second. The standard minimum hello time in seconds is 1 second, which is encoded as 256. Millisecond hello times are encoded using values less than 256; the millisecond hello time equals (x/1000)*256.

When you configure millisecond hellos, the default hello interval of 2 seconds is still used for edge ports; the millisecond hello interval is not used.

Related Commands

forward-delay – changes the wait time before RSTP transitions to the Forwarding state.

max-age – changes the wait time before RSTP refreshes the protocol configuration information.

max-age

Set the time interval for the RSTP bridge to maintain configuration information before refreshing that information.

S5000

Syntax

```
max-age seconds
```

To return to the default values, use the `no max-age` command.

Parameters

max-age	Enter a number of seconds the FTOS waits before refreshing configuration information. The range is 6 to 40 seconds. The default is **20 seconds**.

Defaults **20 seconds**

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

forward-delay – changes the wait time before RSTP transitions to the Forwarding state.

hello-time – changes the time interval between BPDUs.

protocol spanning-tree rstp

Enter RSTP mode to configure RSTP.

S5000

Syntax

```
protocol spanning-tree rstp
```

To exit RSTP mode, use the `exit` command.

Defaults Not configured

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information RSTP is not enabled when you enter RSTP mode. To enable RSTP globally on the system, use the `no disable` command from RSTP mode.

Example

```
FTOS(conf)#protocol spanning-tree rstp
FTOS(config-rstp)##no disable
```

Related Commands disable – disables RSTP globally on the system.

show config

View the current configuration for the mode. Only non-default values are displayed.

S5000

Syntax `show config`

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-rstp)#show config
!
protocol spanning-tree rstp
  no disable
  bridge-priority 16384
```

show spanning-tree rstp

Display the RSTP configuration.

S5000

Syntax `show spanning-tree rstp [brief] [guard]`

Parameters

brief	(OPTIONAL) Enter the keyword `brief` to view a synopsis of the RSTP configuration information.
guard	(OPTIONAL) Enter the keyword `guard` to display the type of guard enabled on an RSTP interface and the current port state.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output from the `show spanning-tree rstp guard` command shown in the Example below.

Field	Description
Interface Name	RSTP interface.
Instance	RSTP instance.

Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), disabled (DIS), or shut down (EDS Shut).
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard)

Example (Brief)

```
FTOS#show spanning-tree rstp brief
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 8192, Address 0001.e805.e306
Root Bridge hello time 4, max age 20, forward delay 15
Bridge ID Priority 16384, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15
Interface                             Designated
Name   PortID Prio Cost Sts Cost      Bridge ID      PortID
---------- ------- --- ------- -------------------- --------
Te 4/0 128.418 128 20000 FWD 20000 16384 0001.e801.6aa8 128.418
Te 4/1 128.419 128 20000 FWD 20000 16384 0001.e801.6aa8 128.419
Te 4/8 128.426 128 20000 FWD 20000 8192 0001.e805.e306 128.130
Te 4/9 128.427 128 20000 BLK 20000 8192 0001.e805.e306 128.131

Interface
Name   Role PortID Prio Cost Sts Cost  Link-type Edge
----------- ---- ------- --- ------- --------- ----
Te 4/0 Desg 128.418 128 20000 FWD 20000 P2P     Yes
Te 4/1 Desg 128.419 128 20000 FWD 20000 P2P     Yes
Te 4/8 Root 128.426 128 20000 FWD 20000 P2P     No
Te 4/9 Altr 128.427 128 20000 BLK 20000 P2P     No
FTOS#
```

Example (EDS, LBK)

NOTE: "LBK_INC" (bold below) means Loopback BPDU Inconsistency.

```
FTOS#show spanning-tree rstp br
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768, Address 0001.e801.6aa8
We are the root
Configured hello time 2, max age 20, forward delay 15

Interface                           Designated
Name   PortID Prio Cost Sts Cost    Bridge ID PortID
- ---- ------- --- ------- -------------------- --------
Te 0/0 128.257 128 20000 EDS 0 32768 0001.e801.6aa8 128.257
Interface
Name   Role PortID    Prio Cost Sts Cost Link-type Edge
--- ------ -------- ---- ------- --- ------- --------- ----
Te 0/0 ErrDis 128.257 128 20000 EDS 0 P2P No

FTOS#show spanning-tree rstp
Root Identifier has priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max
hops 0
Bridge Identifier has priority 32768, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15, max
hops 0
We are the root
Current root has priority 32768, Address 0001.e801.6aa8
Number of topology changes 1, last change occurred 00:00:31
ago on Te 0/0
Port 257 (TenGigabitEthernet 0/0) is LBK_INC Discarding
Port path cost 20000, Port priority 128, Port Identifier
```

```
128.257
Designated root has priority 32768, address 0001.e801.6aa8
Designated bridge has priority 32768, address 0001.e801.6aa8
Designated port id is 128.257, designated path cost 0
Number of transitions to forwarding state 1
BPDU : sent 27, received 9
The port is not in the Edge port mode
```

Example (Guard)

```
FTOS#show spanning-tree rstp guard
Interface
Name   Instance Sts         Guard type
--------- -------- ------------------
Te 0/1 0        INCON(Root) Rootguard
Te 0/2 0        FWD         Loopguard
Te 0/3 0        BLK         Bpduguard
```

spanning-tree rstp

Configure an RSTP interface with one of these settings: port cost, edge port with optional bridge port data unit (BPDU) guard, port priority, loop guard, or root guard.

S5000

Syntax

```
spanning-tree rstp {cost port-cost | edge-port [bpduguard
[shutdown-on-violation]] | priority priority | {loopguard |
rootguard}}
```

Parameters

cost *port-cost*

Enter the keyword `cost` followed by the port cost value. The range is 1 to 200000. The defaults are:

- 1-Gigabit Ethernet interface = **20000**
- 10-Gigabit Ethernet interface = **2000**
- 40-Gigabit Ethernet interface = **2000**
- Port Channel interface with one 1-Gigabit Ethernet = **20000**
- Port Channel interface with one 10-Gigabit Ethernet = **2000**
- Port Channel interface with one 40-Gigabit Ethernet = **2000**
- Port Channel with two 1-Gigabit Ethernet = **18000**
- Port Channel with two 10-Gigabit Ethernet = **1800**
- Port Channel with two 40-Gigabit Ethernet = **1800**

edge-port

Enter the keywords `edge-port` to configure the interface as a rapid spanning tree edge port.

bpduguard

(OPTIONAL) Enter the keyword `portfast` to enable Portfast to move the interface into Forwarding mode immediately after the root fails.

Enter the keyword `bpduguard` to disable the port when it receives a BPDU.

shutdown-on-violation	(OPTIONAL) Enter the keywords `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.
priority ***priority***	Enter keyword `priority` followed by a value in increments of 16 as the priority. The range is 0 to 240. The default is **128**.
loopguard	Enter the keyword `loopguard` to enable loop guard on an RSTP port or port-channel interface.
rootguard	Enter the keyword `rootguard` to enable root guard on an RSTP port or port-channel interface.

Defaults Not configured.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `BPDU guard` option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, or is misconfigured, or is subject to a DOS attack. This option places the port into an Error Disable state if a BPDU appears and a message is logged so that the administrator can take corrective action.

NOTE: A port configured as an edge port, on an RSTP switch, immediately transitions to the Forwarding state. You should only configure ports connected to end-hosts as edge ports. Consider an edge port similar to a port with a `spanning-tree portfast` enabled.

If you do not enable `shutdown-on-violation`, BPDUs are still sent to the stack-unit CPU.

You cannot enable STP root guard and loop guard at the same time on a port. For example, if you configure loop guard on a port on which root guard is already configured, the following error message displays: `% Error: RootGuard is configured. Cannot configure LoopGuard`.

Enabling Portfast BPDU guard and loop guard at the same time on a port results in a port that remains in a Blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an Err-Disabled Blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a Loop-Inconsistent Blocking state and no traffic is forwarded on the port.

Example

```
FTOS(conf)#interface tengigabitethernet 4/0
FTOS(conf-if-te-4/0)#spanning-tree rstp edge-port
FTOS(conf-if-te-4/0)#show config
!
interface TenGigabitEthernet 4/0
  no ip address
  switchport
  spanning-tree rstp edge-port
  no shutdown
FTOS#
```

tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

S5000

Syntax	`tc-flush-standard` To disable, use the `no tc-flush-standard` command.
Defaults	Disabled
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	By default, FTOS implements an optimized flush mechanism for RSTP. This helps in flushing MAC addresses only when necessary (and less often), allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, you can turn on this *knob* command to enable flushing MAC addresses after receiving every topology change notification.

48

Security

The commands in this chapter are available on the S5000 switch.

This chapter contains various types of security commands offered in the Dell Networking operating software (FTOS). The commands are listed in the following sections:

- AAA Accounting Commands
- Authorization and Privilege Commands
- Authentication and Password Commands
- RADIUS Commands
- TACACS+ Commands
- SSH Server and SCP Commands
- Trace List Commands
- Secure DHCP Commands

For configuration details, refer to the Security chapter in the *FTOS Configuration Guide*.

AAA Accounting Commands

AAA Accounting enables tracking of services that users are accessing and the amount of network resources being consumed by those services. When you enable AAA Accounting, the network server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server.

As with authentication and authorization, you must configure AAA Accounting by defining a named list of accounting methods, and then applying that list to various interfaces.

aaa accounting

Enable AAA Accounting and create a record for monitoring the accounting function.

S5000

Syntax `aaa accounting {system | exec | commands level} {name | default}{start-stop | wait-start | stop-only} {tacacs+}`

To disable AAA Accounting, use the `no aaa accounting {system | exec | command level} {name | default}{start-stop | wait-start | stop-only} {tacacs+}` command.

Parameters

system	Enter the keyword `system` to send accounting information of any other AAA configuration.
exec	Enter the keyword `exec` to send accounting information when a user has logged in to EXEC mode.
commands *level*	Enter the keyword `command` followed by a privilege level for accounting of commands executed at that privilege level.
***name* | default**	Enter one of the following: • For `name`, enter a user-defined name of a list of accounting methods. • For `default`, the default accounting methods is used.
start-stop	Enter the keywords `start-stop` to send a “start accounting” notice at the beginning of the requested event and a “stop accounting” notice at the end of the event.
wait-start	Enter the keywords `wait-start` to ensure that the TACACS+ security server acknowledges the start notice before granting the user’s process request.
stop-only	Enter the keywords `stop-only` to instruct the TACACS+ security server to send a “stop record accounting” notice at the end of the requested user process.
tacacs+	Enter the keyword `tacacs+` to use TACACS+ data for accounting. FTOS currently only supports TACACS+ accounting.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

In the example above, TACACS+ accounting is used to track all usage of EXEC command and commands on privilege level 15.

Privilege level 15 is the default. If you want to track usage at privilege level 1 for example, use the `aaa accounting command 1` command.

Example

```
FTOS(conf)# aaa accounting exec default start-stop tacacs+
FTOS(conf)# aaa accounting command 15 default start-stop tacacs
+
FTOS(config)#
```

Related Commands

enable password – changes the password for the `enable` command.

login authentication – enables AAA login authentication on the terminal lines.

password – creates a password.

tacacs-server host – specifies a TACACS+ server host.

aaa accounting suppress

Prevent the generation of accounting records of users with the user name value of NULL.

S5000

Syntax	`aaa accounting suppress null-username` To permit accounting records to users with user name value of NULL, use the `no aaa accounting suppress null-username` command.
Defaults	Accounting records are recorded for all users.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	FTOS issues accounting records for all users on the system, including users whose username string, due to protocol translation, is NULL. For example, a user who comes on line with the `aaa authentication login` *`method-list`* `none` command is applied. Use the `aaa accounting suppress` command to prevent the accounting records from being generated for sessions that do not have user names associated to them.

accounting

Apply an accounting method list to terminal lines.

S5000

Syntax

`accounting {exec | commands` *`level`*`}` *`method-list`*

Parameters

exec	Enter the keyword `exec` to apply an EXEC level accounting method list.
commands *level*	Enter the keywords `commands level` to apply an EXEC and CONFIGURATION level accounting method list.
method-list	Enter a method list that you defined using the `aaa accounting exec` or `aaa accounting` commands.

Defaults	none
Command Modes	LINE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	aaa accounting – enables AAA Accounting and creates a record for monitoring the accounting function.

show accounting

Display the active accounting sessions for each online user.

S5000

Syntax

```
show accounting
```

Defaults none

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This command steps through all active sessions and then displays the accounting records for the active account functions.

Example

```
FTOS#show accounting
Active accounted actions on tty2, User admin Priv 1
  Task ID 1, EXEC Accounting record, 00:00:39 Elapsed,
service=shell
Active accounted actions on tty3, User admin Priv 1
  Task ID 2, EXEC Accounting record, 00:00:26 Elapsed,
service=shell
FTOS#
```

Related Commands aaa accounting – enables AAA Accounting and creates a record for monitoring the accounting function.

Authorization and Privilege Commands

Use the following commands to set the `command line authorization` and `privilege levels`.

aaa authorization commands

Set parameters that restrict (or permit) a user's access to EXEC and CONFIGURATION level commands.

S5000

Syntax

```
aaa authorization commands level {name | default} {local ||
tacacs+ || none}
```

Undo a configuration with the `no aaa authorization commands level {name | default} {local || tacacs+ || none}` command.

Parameters

commands *level*	Enter the keyword `commands` followed by the command privilege level for command level authorization.

name	Define a name for the list of authorization methods.
default	Define the default list of authorization methods.
local	Use the authorization parameters on the system to perform authorization.
tacacs+	Use the TACACS+ protocol to perform authorization.
none	Enter the keyword `none` to apply no authorization.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

aaa authorization config-commands

Set parameters that restrict (or permit) a user’s access to EXEC level commands.

S5000

Syntax `aaa authorization config-commands`

Disable authorization checking for CONFIGURATION level commands using the `no aaa authorization config-commands` command.

Defaults Enabled when you configure `aaa authorization commands` command.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information By default, the `aaa authorization commands` command configures the system to check both EXEC level and CONFIGURATION level commands. Use the command `no aaa authorization config-commands` to enable only EXEC-level command checking.

aaa authorization exec

Set parameters that restrict (or permit) a user’s access to EXEC-level commands.

S5000

Syntax

```
aaa authorization exec {name | default} {local || tacacs+ ||
if-authenticated || none}
```

To disable authorization checking for EXEC level commands, use the `no aaa authorization exec` command.

Parameters

name	Define a name for the list of authorization methods.
default	Define the default list of authorization methods.
local	Use the authorization parameters on the system to perform authorization.
tacacs+	Use the TACACS+ protocol to perform authorization.
none	Enter the keyword `none` to apply no authorization.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

authorization

Apply an authorization method list to terminal lines.

S5000

Syntax

```
authorization {exec | commands level} method-list
```

Parameters

exec	Enter the keyword `exec` to apply an EXEC level accounting method list.
commands *level*	Enter the keywords `commands level` to apply an EXEC and CONFIGURATION level accounting method list.
method-list	Enter a method list that you defined using the `aaa accounting exec` or `aaa accounting` commands.

Defaults none

Command Modes LINE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

aaa authorization commands – sets the parameters that restrict (or permit) a user's access to EXEC and CONFIGURATION level commands

aaa authorization exec – sets the parameters that restrict (or permit) a user's access to EXEC level commands.

privilege level (CONFIGURATION mode)

Change the access or privilege level of one or more commands.

S5000

Syntax

`privilege mode {level level command | reset command}`

To delete access to a level and command, use the `no privilege mode level level command` command.

Parameters

mode	Enter one of the following keywords as the mode for which you are controlling access: • `configure` for CONFIGURATION mode • `exec` for EXEC mode • `interface` for INTERFACE modes • `line` for LINE mode • `route-map` for ROUTE-MAP mode • `router` for ROUTER OSPF, ROUTER RIP, ROUTER ISIS and ROUTER BGP modes
level *level*	Enter the keyword `level` followed by a number for the access level. The range is 0 to 15. Level 1 is EXEC mode and Level 15 allows access to all CLI modes and commands.
reset	Enter the keyword `reset` to return the security level to the default setting.
command	Enter the command's keywords to assign the command to a certain access level. You can enter one or all of the keywords.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `enable password` command to define a password for the level to which you are assigning privilege or access.

privilege level (LINE mode)

Change the access level for users on the terminal lines.

S5000

Syntax

`privilege level level`

To delete access to a terminal line, use the `no privilege level level` command.

Parameters

level *level*	Enter the keyword `level` followed by a number for the access level. The range is 0 to 15. Level 1 is EXEC mode and Level 15 allows access to all CLI modes.

Defaults

level = 15

Command Modes

LINE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Authentication and Password Commands

Use the following the commands to manage access to the system

aaa authentication enable

Configure AAA Authentication method lists for user access to EXEC privilege mode (the “Enable” access).

S5000

Syntax

`aaa authentication enable {default | method-list-name} method [... method2]`

To return to the default setting, use the `no aaa authentication enable {default | method-list-name} method [... method2]` command.

Parameters

default	Enter the keyword `default` followed by the authentication methods to use as the default sequence of methods to be used for the Enable log-in. The default is `default enable`.
method-list-name	Enter a text string (up to 16 characters long) to name the list of enabled authentication methods activated at log in.
method	Enter one of the following methods:

- `enable` - use the password defined by the `enable password` command in CONFIGURATION mode.
- `line` - use the password defined by the `password` command in LINE mode.
- `none` - no authentication.
- `radius` - use the RADIUS server(s) configured with the `radius-server host` command.
- `tacacs+` - use the TACACS+ server(s) configured with the `tacacs-server host` command.

... method2	(OPTIONAL) In the event of a "no response" from the first method, FTOS applies the next configured method.

Defaults

Use the `enable` password.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

By default, the `Enable password` is used. If you configure `aaa authentication enable default`, FTOS uses the methods defined for `Enable access` instead.

Methods configured with the `aaa authentication enable` command are evaluated in the order they are configured. If authentication fails using the primary method, FTOS employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, FTOS proceeds to the next authentication method. The TACACS+ is incorrect, but the user is still authenticated by the secondary method.

Related Commands

enable password – changes the password for the `enable` command.

login authentication – enables AAA login authentication on the terminal lines.

password – creates a password.

radius-server host – specifies a RADIUS server host.

tacacs-server host – specifies a TACACS+ server host.

aaa authentication login

Configure AAA Authentication method lists for user access to EXEC mode (`Enable log-in`).

S5000

Syntax

`aaa authentication login {method-list-name | default} method [... method4]`

To return to the default setting, use the `no aaa authentication login {method-list-name | default}` command.

Parameters

method-list-name	Enter a text string (up to 16 characters long) as the name of a user-configured method list that can be applied to different lines.
default	Enter the keyword `default` to specify that the method list specified is the default method for all terminal lines.
method	Enter one of the following methods: • `enable` - use the password defined by the `enable password` command in CONFIGURATION mode. • `line` - use the password defined by the `password` command in LINE mode. • `none` - no authentication. • `radius` - use the RADIUS server(s) configured with the `radius-server host` command. • `tacacs+` - use the TACACS+ server(s) configured with the `tacacs-server host` command.
... method4	(OPTIONAL) Enter up to four additional methods. In the event of a “no response” from the first method, FTOS applies the next configured method (up to four configured methods).

Defaults

Not configured (that is, no authentication is performed).

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

By default, the locally configured username password is used. If you configure `aaa authentication login default`, FTOS uses the methods defined by this command for login instead.

Methods configured with the `aaa authentication login` command are evaluated in the order they are configured. If users encounter an error with the first method listed, FTOS applies the next method configured. If users fail the first method listed, no other methods are applied. The only exception is the local method. If the user’s name is not listed in the local database, the next method is applied. If the correct user name/password combination are not entered, the user is not allowed access to the switch.

NOTE: If authentication fails using the primary method, FTOS employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, FTOS proceeds to the next authentication method. The TACACS+ is incorrect, but the user is still authenticated by the secondary method.

After configuring the `aaa authentication login` command, configure the `login authentication` command to enable the authentication scheme on terminal lines.

Connections to the SSH server work with the following login mechanisms: local, radius, and tacacs.

Related Commands

login authentication – enables AAA login authentication on the terminal lines.

password – creates a password.

radius-server host – specifies a RADIUS server host.

tacacs-server host – specifies a TACACS+ server host.

access-class

Restrict incoming connections to a particular IP address in a defined IP access control list (ACL).

S5000

Syntax

`access-class access-list-name`

To delete a setting, use the `no access-class` command.

Parameters

access-list-name	Enter the name of an established IP Standard ACL.

Defaults

Not configured.

Command Modes

LINE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

line – applies an authentication method list to the designated terminal lines.

ip access-list standard – names (or selects) a standard access list to filter based on the IP address.

ip access-list extended – names (or selects) an extended access list based on the IP addresses or protocols.

enable password

Change the password for the `enable` command.

S5000

Syntax

`enable password [level level] [encryption-type] password`

To delete a password, use the `no enable password [encryption-type] password [level level]` command.

Parameters

level *level*	(OPTIONAL) Enter the keyword `level` followed by a number as the level of access. The range is from 1 to 15.
encryption-type	(OPTIONAL) Enter the number `7` or `0` as the encryption type. Enter a `7` followed by a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router.

	Use this parameter only with a password that you copied from the `show running-config` file of another Dell Networking router.
password	Enter a text string, up to 32 characters long, as the clear text password.

Defaults No password is configured. *level* = **15**.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use this command to define a password for a level and use the `privilege level (CONFIGURATION mode)` command to control access to command modes.

Passwords must meet the following criteria:

- Start with a letter, not a number.
- Passwords can have a regular expression as the password. To create a password with a regular expression in it, you must use CNTL + v prior to entering regular expression. For example, to create the password `abcd]e`, you type “`abcd CNTL v ]e`”. When the password is created, you do not use the CNTL + v key combination and enter “`abcd]e`”.

NOTE: The question mark (?) and the tilde (~) are not supported characters.

Related Commands

show running-config – views the current configuration.

privilege level (CONFIGURATION mode) – controls access to the command modes within the switch.

enable restricted

Allows Dell Networking technical support to access restricted commands.

S5000

Syntax `enable restricted [encryption-type] password`

To disallow access to restricted commands, use the `no enable restricted` command.

Parameters

encryption-type	(OPTIONAL) Enter the number `7` as the encryption type. Enter `7` followed a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router. Use this parameter only with a password that you copied from the `show running-config` file of another Dell Networking router.
password	Enter a text string, up to 32 characters long, as the clear text password.

Defaults Not configured.

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Only Dell Networking Technical Support staff use this command.

enable secret

Change the password for the `enable` command.

S5000

Syntax `enable secret [level` *`level`*`] [`*`encryption-type`*`]` *`password`*

To delete a password, use the `no enable secret [`*`encryption-type`*`]` *`password`* `[level` *`level`*`]` command.

Parameters

level ***level***	(OPTIONAL) Enter the keyword `level` followed by a number as the level of access. The range is from 1 to 15.
encryption-type	(OPTIONAL) Enter the number `5` or `0` as the encryption type. Enter a `5` followed by a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router. Use this parameter only with a password that you copied from the `show running-config` file of another Dell Networking router.
password	Enter a text string, up to 32 characters long, as the clear text password.

Defaults No password is configured. *level* = **15**.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Use this command to define a password for a level and use the `privilege level (CONFIGURATION mode)` command to control access to command modes.

Passwords must meet the following criteria:

- Start with a letter, not a number.
- Passwords can have a regular expression as the password. To create a password with a regular expression in it, you must use CNTL + v prior to entering regular expression. For example, to create the password `abcd]e`, you type "`abcd CNTL v ]e`". When the password is created, you do not use the CNTL + v key combination and enter "`abcd]e`".

NOTE: The question mark (?) and the tilde (~) are not supported characters.

Related Commands

show running-config – views the current configuration.

privilege level (CONFIGURATION mode) – controls access to the command modes within the switch.

login authentication

Apply an authentication method list to designated the terminal lines.

S5000

Syntax

`login authentication {method-list-name | default}`

To use the local user/password database for login authentication, use the `no login authentication` command.

Parameters

method-list-name	Enter the keywords `method-list-name` to specify that method list, created in the `aaa authentication login` command, to be applied to the designated terminal line.
default	Enter the keyword `default` to specify that the default method list, created in the `aaa authentication login` command, is applied to the terminal line.

Defaults

No authentication is performed on the console lines. Local authentication is performed on the virtual terminal and auxiliary lines.

Command Modes

LINE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you configure the `aaa authentication login default` command, the `login authentication default` command automatically is applied to all terminal lines.

Related Commands

aaa authentication login – selects the login authentication methods.

password

Specify a password for users on terminal lines.

S5000

Syntax	`password [`*`encryption-type`*`]` *`password`* To delete a password, use the `no password` *`password`* command.

Parameters

encryption-type	(OPTIONAL) Enter either zero (`0`) or `7` as the encryption type for the password entered. The options are • `0` is the default and means the password is not encrypted and stored as clear text. • `7` means that the password is encrypted and hidden.
password	Enter a text string up to 32 characters long. The first character of the password must be a letter. You cannot use spaces in the password.

Defaults No password is configured.

Command Modes LINE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information FTOS prompts users for these passwords when the method for authentication or authorization used is "line".

Related Commands

enable password – sets the password for the `enable` command.

login authentication – configures an authentication method to log in to the switch.

service password-encryption – encrypts all passwords configured in FTOS.

radius-server key – configures a key for all RADIUS communications between the switch and the RADIUS host server.

tacacs-server key – configures a key for communication between a TACACS+ server and client.

username – establishes an authentication system based on user names.

password-attributes

Configure the password attributes (strong password).

S5000

Syntax

```
password-attributes [min-length number] [max-retry number]
[character-restriction [upper number] [lower number] [numeric
number] [special-char number]]
```

To return to the default, use the `no password-attributes [min-length *number*] [max-retry *number*] [character-restriction [upper *number*] [lower *number*] [numeric *number*] [special-char *number*]]` command.

Parameters

min-length *number*	(OPTIONAL) Enter the keywords `min-length` followed by the number of characters. The range is 0 to 32 characters.
max-retry *number*	(OPTIONAL) Enter the keywords `max-retry` followed by the number of maximum password retries. The range is 0 to 16.
character-restriction	(OPTIONAL) Enter the keywords `character-restriction` to indicate a character restriction for the password.
upper *number*	(OPTIONAL) Enter the keyword `upper` followed the upper number. The range is 0 to 31.
lower *number*	(OPTIONAL) Enter the keyword `lower` followed the lower number. The range is 0 to 31.
numeric *number*	(OPTIONAL) Enter the keyword `numeric` followed the numeric number. The range is 0 to 31.
special-char *number*	(OPTIONAL) Enter the keywords `special-char` followed the number of special characters permitted. The range is 0 to 31.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands password – specifies a password for users on terminal lines.

privilege level (CONFIGURATION mode)

Change the access or privilege level of one or more commands.

S5000

Syntax `privilege *mode* {level *level command* | reset *command*}`

To delete access to a level and command, use the `no privilege mode level level command` command.

Parameters

mode	Enter one of the following keywords as the mode for which you are controlling access: • `configure` for CONFIGURATION mode • `exec` for EXEC mode

- `interface` for INTERFACE modes
- `line` for LINE mode
- `route-map` for ROUTE-MAP mode
- `router` for ROUTER OSPF, ROUTER RIP, ROUTER ISIS and ROUTER BGP modes

level *level*	Enter the keyword `level` followed by a number for the access level. The range is 0 to 15. Level 1 is EXEC mode and Level 15 allows access to all CLI modes and commands.
reset	Enter the keyword `reset` to return the security level to the default setting.
command	Enter the command's keywords to assign the command to a certain access level. You can enter one or all of the keywords.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Use the `enable password` command to define a password for the level to which you are assigning privilege or access.

privilege level (LINE mode)

Change the access level for users on the terminal lines.

S5000

Syntax `privilege level` *`level`*

To delete access to a terminal line, use the `no privilege level` *`level`* command.

Parameters

level *level*	Enter the keyword `level` followed by a number for the access level. The range is 0 to 15. Level 1 is EXEC mode and Level 15 allows access to all CLI modes.

Defaults *level* = 15

Command Modes LINE

Command History

Version 9.0(1.3)	Introduced on the S5000.

service password-encryption

Encrypt all passwords configured in FTOS.

S5000

Syntax `service password-encryption`

To store new passwords as clear text, use the `no service password-encryption` command.

Defaults Enabled.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

CAUTION: Encrypting passwords with this command does not provide a high level of security. When the passwords are encrypted, you cannot return them to plain text unless you re-configure them. To remove an encrypted password, use the `no password password` command.

To keep unauthorized people from viewing passwords in the switch configuration file, use the `service password-encryption` command. This command encrypts the clear-text passwords created for user name passwords, authentication key passwords, the privileged command password, and console and virtual terminal line access passwords.

To view passwords, use the `show running-config` command.

show privilege

View your access level.

S5000

Syntax `show privilege`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show privilege
Current privilege level is 15
FTOS#
```

Related Commands	privilege level (CONFIGURATION mode) – assigns access control to different command modes.

show users

Allows you to view information on all users logged into the switch.

S5000

Syntax `show users [all]`

Parameters

all	(OPTIONAL) Enter the keyword `all` to view all terminal lines in the switch.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The following describes output from the `show user` command shown in the Example below.

Field	**Description**
(untitled)	Indicates with an asterisk (*) which terminal line you are using.
Line	Displays the terminal lines currently in use.
User	Displays the user name of all users logged in.
Host(s)	Displays the terminal line status.
Location	Displays the IP address of the user.

Example

```
FTOS#show user
Line          User   Host(s)  Location
0 console 0   admin  idle
* 3 vty 1     admin  idle     172.31.1.4
FTOS#
```

Related Commands username – enables a user.

timeout login response

Specify how long the software waits for the login input (for example, the user name and password) before timing out.

S5000

Syntax

`timeout login response seconds`

To return to the default values, use the `no timeout login response` command.

Parameters

seconds	Enter a number of seconds the software waits before logging you out. The range is: • VTY: 1 to 30 seconds, the default is **30 seconds**. • Console: 1 to 300 seconds, the default is **0 seconds** (no timeout). • AUX: 1 to 300 seconds, the default is **0 seconds** (no timeout).

Defaults

See above.

Command Modes

LINE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The software measures the period of inactivity defined in this command as the period between consecutive keystrokes. For example, if your password is “password” you can enter “p” and wait 29 seconds to enter the next letter.

username

Establish an authentication system based on user names.

S5000

Syntax

`username name [access-class access-list-name] [nopassword | {password | secret} [encryption-type] password] [privilege level]`

If you do not want a specific user to enter a password, use the `nopassword` option.

To delete authentication for a user, use the `no username name` command.

Parameters

name	Enter a text string for the name of the user up to 63 characters.
access-class *access-list-name*	Enter the keywords `access-class` followed by the name of a configured access control list (either a IP access control list or MAC access control list).
nopassword	Enter the keyword `nopassword` to specify that the user should not enter a password.

password	Enter the keyword `password` followed by the `encryption-type` or the password.
secret	Enter the keyword `secret` followed by the `encryption-type` or the password.
encryption-type	Enter an encryption type for the `password` that you will enter. • `0` directs FTOS to store the password as clear text. It is the default encryption type when using the `password` option. • `7` to indicate that a password encrypted using a DES hashing algorithm will follow. This encryption type is available with the `password` option only. • `5` to indicate that a password encrypted using an MD5 hashing algorithm will follow. This encryption type is available with the `secret` option only, and is the default encryption type for this option.
password	Enter a string up to 32 characters long.
privilege *level*	Enter the keyword `privilege` followed by a number from zero (0) to 15.
secret	Enter the keyword `secret` followed by the encryption type.

Defaults

The default encryption type for the `password` option is **0**. The default encryption type for the `secret` option is **0**.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To view the defined user names, use the `show running-config user` command.

Related Commands

password – specifies a password for users on terminal lines.

show running-config – views the current configuration.

RADIUS Commands

FTOS supports the following RADIUS commands.

debug radius

View RADIUS transactions to assist with troubleshooting.

S5000

Syntax	`debug radius` To disable debugging of RADIUS, use the `no debug radius` command.
Defaults	Disabled.
Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ip radius source-interface

Specify an interface's IP address as the source IP address for RADIUS connections.

S5000

Syntax

`ip radius source-interface interface`

To delete a source interface, use the `no ip radius source-interface` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information. • For Loopback interfaces, enter the keyword `loopback` followed by a number from zero (0) to 16838. • For the Null interface, enter the keywords `null 0`. • For a Port Channel interface, enter the keywords `port-channel` followed by a number. The range is 1 to 128. • For VLAN interface, enter the keyword `vlan` followed by a number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

radius-server deadtime

Configure a time interval during which non-responsive RADIUS servers to authentication requests are skipped.

S5000

Syntax `radius-server deadtime` *`seconds`*

To disable this function or return to the default value, use the `no radius-server deadtime` command.

Parameters

seconds	Enter a number of seconds during which non-responsive RADIUS servers are skipped. The range is 0 to 2147483647 seconds. The default is **0 seconds**.

Defaults **0 seconds**

Command Modes CONFIGURATION

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

radius-server host

Configure a RADIUS server host.

S5000

Syntax

```
radius-server host {hostname | ipv4-address | ipv6-address}
[auth-port port-number] [retransmit retries] [timeout seconds]
[key [encryption-type] key]
```

Parameters

hostname	Enter the name of the RADIUS server host.
ipv4-address* | *ipv6-address	Enter the IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X) of the RADIUS server host.
auth-port *port-number*	(OPTIONAL) Enter the keywords `auth-port` followed by a number as the port number. The range is zero (0) to 65535. The default port-number is **1812**.
retransmit *retries*	(OPTIONAL) Enter the keyword `retransmit` followed by a number as the number of attempts. This parameter overwrites the `radius-`

	`server retransmit` command. The range is zero (0) to 100. The default is **3 attempts**.
timeout *seconds*	(OPTIONAL) Enter the keyword `timeout` followed by the seconds the time interval the switch waits for a reply from the RADIUS server. This parameter overwrites the `radius-server timeout` command. The range is 0 to 1000. The default is **5 seconds**.
key [*encryption-type*] *key*	(OPTIONAL) Enter the keyword `key` followed by an optional encryption-type and a string up to 42 characters long as the authentication key. This authentication key is used by the RADIUS host server and the RADIUS daemon operating on this switch. For the encryption-type, enter either zero (`0`) or `7` as the encryption type for the key entered. The options are: • `0` is the default and means the password is not encrypted and stored as clear text. • `7` means that the password is encrypted and hidden. Configure this parameter last because leading spaces are ignored.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use this command to configure any number of RADIUS server hosts for each server host that is configured. FTOS searches for the RADIUS hosts in the order they are configured in the software.

The global default values for the `timeout`, `retransmit`, and `key` optional parameters are applied, unless those values are specified in the `radius-server host` or other commands. If you configure the `timeout`, `retransmit`, or `key` values, you must include those keywords when using the `no radius-server host` command syntax to return to the global default values.

Related Commands

login authentication – sets the database to be checked when a user logs in.

radius-server key – sets an authentication key for RADIUS communications.

radius-server retransmit – sets the number of times the RADIUS server attempts to send information.

radius-server timeout – sets the time interval before the RADIUS server times out.

radius-server key

Configure a key for all RADIUS communications between the switch and the RADIUS host server.

S5000

Syntax

`radius-server key [`*`encryption-type`*`]` *`key`*

To delete a password, use the `no radius-server key` command.

Parameters

encryption-type	(OPTIONAL) Enter either zero (`0`) or `7` as the encryption type for the key entered. The options are: • `0` is the default and means the key is not encrypted and stored as clear text. • `7` means that the key is encrypted and hidden.
key	Enter a string that is the key to be exchanged between the switch and RADIUS servers. It can be up to 42 characters long.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The key configured on the switch must match the key configured on the RADIUS server daemon.

If you configure the `key` parameter in the `radius-server host` command, the key configured with the `radius-server key` command is the default key for all RADIUS communications.

Related Commands

radius-server host – configures a RADIUS host.

radius-server retransmit

Configure the number of times the switch attempts to connect with the configured RADIUS host server before declaring the RADIUS host server unreachable.

S5000

Syntax

`radius-server retransmit` *`retries`*

To configure zero retransmit attempts, use the `no radius-server retransmit` command.

To return to the default setting, use the `radius-server retransmit 3` command.

Parameters

retries	Enter a number of attempts that FTOS tries to locate a RADIUS server. The range is zero (0) to 100. The default is **3 retries**.

Defaults 3 retries

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands radius-server host – configures a RADIUS host.

radius-server timeout

Configure the amount of time the RADIUS client (the switch) waits for a RADIUS host server to reply to a request.

S5000

Syntax `radius-server timeout seconds`

To return to the default value, use the `no radius-server timeout` command.

Parameters

seconds	Enter the number of seconds between an unsuccessful attempt and the FTOS times out. The range is zero (0) to 1000 seconds. The default is **5 seconds**.

Defaults 5 seconds

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands radius-server host – configures a RADIUS host.

TACACS+ Commands

FTOS supports TACACS+ as an alternate method for login authentication.

debug tacacs+

View TACACS+ transactions to assist with troubleshooting.

S5000

Syntax

```
debug tacacs+
```

To disable debugging of TACACS+, use the `no debug tacacs+` command.

Defaults Disabled.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip tacacs source-interface

Specify an interface's IP address as the source IP address for TACACS+ connections.

S5000

Syntax

```
ip tacacs source-interface interface
```

To delete a source interface, use the `no ip tacacs source-interface` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For Loopback interfaces, enter the keyword `loopback` followed by a number from zero (0) to 16838. • For the Null interface, enter the keywords `null 0`. • For a Port Channel interface, enter the keywords `port-channel` followed by a number. The range is 1 to 128. • For a Ten Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information. • For VLAN interface, enter the keyword `vlan` followed by a number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

tacacs-server host

Specify a TACACS+ host.

S5000

Syntax

```
tacacs-server host {hostname | ipv4-address | ipv6-address}
[port number] [timeout seconds] [key key]
```

Parameters

hostname	Enter the name of the TACACS+ server host.
ipv4-address* | *ipv6-address	Enter the IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X) of the TACACS+ server host.
port *number*	(OPTIONAL) Enter the keyword `port` followed by a number as the port to be used by the TACACS+ server. The range is zero (0) to 65535. The default is **49**.
timeout *seconds*	(OPTIONAL) Enter the keyword `timeout` followed by the number of seconds the switch waits for a reply from the TACACS+ server. The range is 0 to 1000. The default is **10 seconds**.
key *key*	(OPTIONAL) Enter the keyword `key` followed by a string up to 42 characters long as the authentication key. This authentication key must match the key specified in the `tacacs-server key` for the TACACS+ daemon.

Defaults Not configured.

Command Modes CONFIGURATION

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To list multiple TACACS+ servers to be used by the `aaa authentication login` command, configure this command multiple times.

If you are not configuring the switch as a TACACS+ server, you do not need to configure the `port`, `timeout` and `key` optional parameters. If you do not configure a key, the key assigned in the `tacacs-server key` command is used.

Related Commands

aaa authentication login – specifies the login authentication method.

tacacs-server key – configures a TACACS+ key for the TACACS server.

tacacs-server key

Configure a key for communication between a TACACS+ server and a client.

S5000

Syntax	`tacacs-server key [`*`encryption-type`*`] key` To delete a key, use the `no tacacs-server key` *`key`* command.
Parameters	*encryption-type*: (OPTIONAL) Enter either zero (`0`) or `7` as the encryption type for the key entered. The options are: • `0` is the default and means the key is not encrypted and stored as clear text. • `7` means that the key is encrypted and hidden. *key*: Enter a text string, up to 42 characters long, as the clear text password. Leading spaces are ignored.
Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)**: Introduced on the S5000.
Usage Information	The key configured with this command must match the key configured on the TACACS+ daemon.

Port Authentication (802.1X) Commands

An authentication server must authenticate a client connected to an 802.1X switch port. Until the authentication, only Extensible Authentication Protocol over LAN (EAPOL) traffic is allowed through the port to which a client is connected. After authentication is successful, normal traffic passes through the port.

FTOS supports RADIUS and Active Directory environments using 802.1X Port Authentication.

Important Points to Remember

FTOS limits network access for certain users by using VLAN assignments. 802.1X with VLAN assignment has these characteristics when configured on the switch and the RADIUS server.

- 802.1X is supported on the S5000.
- 802.1X is not supported on the LAG or the channel members of a LAG.
- If no VLAN is supplied by the RADIUS server or if 802.1X authorization is disabled, the port is configured in its access VLAN after successful authentication.
- If 802.1X authorization is enabled but the VLAN information from the RADIUS server is not valid, the port returns to the Unauthorized state and remains in the configured access VLAN. This prevents ports from appearing unexpectedly in an inappropriate VLAN due to a configuration error. Configuration errors create an entry in Syslog.

- If 802.1X authorization is enabled and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.
- If port security is enabled on an 802.1X port with VLAN assignment, the port is placed in the RADIUS server assigned VLAN.
- If 802.1X is disabled on the port, it is returned to the configured access VLAN.
- When the port is in the Force Authorized, Force Unauthorized, or Shutdown state, it is placed in the configured access VLAN.
- If an 802.1X port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration does not take effect.
- The 802.1X with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN membership.

dot1x authentication (Configuration)

Enable dot1x globally; dot1x must be enabled both globally and at the interface level.

S5000

Syntax

```
dot1x authentication
```

To disable dot1x on an globally, use the `no dot1x authentication` command.

Defaults Disabled.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands dot1x authentication (Interface) – enables dot1x on an interface.

dot1x authentication (Interface)

Enable dot1x on an interface; dot1x must be enabled both globally and at the interface level.

S5000

Syntax

```
dot1x authentication
```

To disable dot1x on an interface, use the `no dot1x authentication` command.

Defaults Disabled.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

dot1x authentication (Configuration) – enables dot1x globally.

dot1x auth-fail-vlan

Configure an authentication failure VLAN for users and devices that fail 802.1X authentication.

S5000

Syntax

`dot1x auth-fail-vlan vlan-id [max-attempts number]`

To delete the authentication failure VLAN, use the `no dot1x auth-fail-vlan vlan-id [max-attempts number]` command.

Parameters

vlan-id	Enter the VLAN Identifier. The range is 1 to 4094.
max-attempts *number*	(OPTIONAL) Enter the keywords `max-attempts` followed number of attempts desired before authentication fails. The range is 1 to 5. The default is **3**.

Defaults

3 attempts

Command Modes

CONFIGURATION (conf-if-interface-slot/port)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If the host responds to 802.1X with an incorrect login/password, the login fails. The switch attempts to authenticate again until the maximum attempts configured is reached. If the authentication fails after all allowed attempts, the interface is moved to the authentication failed VLAN.

After the authentication VLAN is assigned, the port-state must be toggled to restart authentication. Authentication occurs at the next re-authentication interval (`dot1x reauthentication`).

Related Commands

dot1x port-control – enables port-control on an interface.

dot1x guest-vlan – configures a guest VLAN for non-dot1x devices.

show dot1x interface – displays the 802.1X information on an interface.

dot1x auth-server

Configure the authentication server to RADIUS.

S5000

Syntax	`dot1x auth-server radius`
Defaults	none
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.

dot1x guest-vlan

Configure a guest VLAN for limited access users or for devices that are not 802.1X capable.

S5000

Syntax

`dot1x guest-vlan vlan-id`

To disable the guest VLAN, use the `no dot1x guest-vlan vlan-id` command.

Parameters

vlan-id	Enter the VLAN Identifier. The range is 1 to 4094.

Defaults

Not configured.

Command Modes

CONFIGURATION (conf-if-interface-slot/port)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

802.1X authentication is enabled when an interface is connected to the switch. If the host fails to respond within a designated amount of time, the authenticator places the port in the guest VLAN.

If a device does not respond within 30 seconds, it is assumed that the device is not 802.1X capable. Therefore, a guest VLAN is allocated to the interface and authentication for the device occurs at the next re-authentication interval (`dot1x reauthentication`).

If the host fails authentication for the designated amount of times, the authenticator places the port in authentication failed VLAN (`dot1x auth-fail-vlan`).

NOTE: The layer 3 portion of guest VLAN and authentication fail VLANs can be created regardless if the VLAN is assigned to an interface or not. After an interface is assigned a guest VLAN (which has an IP address), routing through the guest VLAN is the same as any other traffic. However, the interface may join/leave a VLAN dynamically.

Related Commands	dot1x auth-fail-vlan – configures a VLAN for authentication failures. dot1x reauthentication – enables periodic re-authentication. show dot1x interface – displays the 802.1X information on an interface.

dot1x max-eap-req

Configure the maximum number of times an extensive authentication protocol (EAP) request is transmitted before the session times out.

S5000

Syntax

```
dot1x max-eap-req number
```

To return to the default, use the `no dot1x max-eap-req` command.

Parameters

number	Enter the number of times an EAP request is transmitted before a session time-out. The range is 1 to 10. The default is **2**.

Defaults 2

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands interface range – configures a range of interfaces.

dot1x port-control

Enable port control on an interface.

S5000

Syntax

```
dot1x port-control {force-authorized | auto | force-
unauthorized}
```

Parameters

force-authorized	Enter the keywords `force-authorized` to forcibly authorize a port.
auto	Enter the keyword `auto` to authorize a port based on the 802.1X operation result.
force-unauthorized	Enter the keywords `force-unauthorized` to forcibly de-authorize a port.

Defaults	none
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	The authenticator performs authentication only when `port-control` is set to `auto`.

dot1x quiet-period

Set the number of seconds that the authenticator remains quiet after a failed authentication with a client.

S5000

Syntax

`dot1x quiet-period seconds`

To disable quiet time, use the `no dot1x quiet-time` command.

Parameters

seconds	Enter the number of seconds. The range is 1 to 65535. The default is **30**.

Defaults **30 seconds**

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

dot1x reauthentication

Enable periodic re-authentication of the client.

S5000

Syntax

`dot1x reauthentication [interval seconds]`

To disable periodic re-authentication, use `the no dot1x reauthentication` command.

Parameters

interval *seconds*	(Optional) Enter the keyword `interval` followed by the interval time, in seconds, after which re-authentication will be initiated. The range is 1 to 31536000 (1 year). The default is**3600 (1 hour)**.

Defaults **3600 seconds (1 hour)**

Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	interface range – configures a range of interfaces.

dot1x reauth-max

Configure the maximum number of times a port can re-authenticate before the port becomes unauthorized.

S5000

Syntax

`dot1x reauth-max` *`number`*

To return to the default, use the `no dot1x reauth-max` command.

Parameters

number	Enter the permitted number of re-authentications. The range is 1 - 10. The default is **2**.

Defaults 2

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

dot1x server-timeout

Configure the amount of time after which exchanges with the server time out.

S5000

Syntax

`dot1x server-timeout` *`seconds`*

To return to the default, use the `no dot1x server-timeout` command.

Parameters

seconds	Enter a time-out value in seconds. The range is 1 to 300, where 300 is implementation dependant. The default is **30**.

Defaults 30 seconds

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

dot1x supplicant-timeout

Configure the amount of time after which exchanges with the supplicant time out.

S5000

Syntax `dot1x supplicant-timeout` *`seconds`*

To return to the default, use the`no dot1x supplicant-timeout` command.

Parameters

seconds	Enter a time-out value in seconds. The range is 1 to 300, where 300 is implementation dependant. The default is **30**.

Defaults **30 seconds**

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

dot1x tx-period

Configure the intervals at which EAPOL PDUs are transmitted by the Authenticator PAE.

S5000

Syntax `dot1x tx-period` *`seconds`*

To return to the default, use the `no dot1x tx-period` command.

Parameters

seconds	Enter the interval time, in seconds, that EAPOL PDUs are transmitted. The range is 1 to 31536000 (1 year). The default is **30**.

Defaults **30 seconds**

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

show dot1x interface

Display the 802.1X information on an interface.

S5000

Syntax	`show dot1x interface` *`interface`*

Parameters

interface	Enter one of the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.

Defaults none

Command Modes

- EXEC
- EXEC privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show dot1x int  Te 2/32
802.1x information on   Te 2/32:
-----------------------------
Dot1x Status:           Enable
Port Control:           AUTO
Port Auth Status:       UNAUTHORIZED
Re-Authentication:      Disable
Untagged VLAN id:       None
Guest VLAN:             Enable
Guest VLAN id:          10
Auth-Fail VLAN:         Enable
Auth-Fail VLAN id:      11
Auth-Fail Max-Attempts: 3
Tx Period:              30 seconds
Quiet Period:           60 seconds
ReAuth Max:             2
Supplicant Timeout:     30 seconds
Server Timeout:         30 seconds
Re-Auth Interval:       3600 seconds
Max-EAP-Req:            2
Auth Type:              SINGLE_HOST
Auth PAE State:         Initialize
Backend State:          Initialize
FTOS#
```

SSH Server and SCP Commands

FTOS supports secure shell (SSH) protocol versions 1.5 and 2.0. SSH is a protocol for secure remote login over an insecure network. SSH sessions are encrypted and use authentication.

crypto key generate

Generate keys for the SSH server.

S5000

Syntax

NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

```
crypto key generate {rsa | rsa1}
```

Parameters

rsa	Enter the keyword `rsa` followed by the key size to generate a SSHv2 RSA host keys. The range is 1024 to 2048 if you did not enable FIPS mode; if you enabled FIPS mode, you can only generate a 2048-bit key. The default is **1024**. **NOTE:** You must have a license to access the FIPS mode. For more information, contact your Dell Networking representative.
rsa1	Enter the keyword `rsa1` followed by the key size to generate a SSHv1 RSA host keys. The range is 1024 to 2048. The default is **1024**. **NOTE:** This option is not available in FIPS mode.

Defaults Key size **1024**; if you enable FIPS mode, the key size is **2048**.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The host keys are required for key-exchange by the SSH server. If the keys are not found when you enable the server (`ip ssh server enable`), the keys are automatically generated.

This command requires user interaction and generates a prompt prior to overwriting any existing host keys.

NOTE: Only a user with superuser permissions should generate host-keys.

Example

```
FTOS#conf
FTOS(conf)#crypto key generate rsa1
Enter key size <1024-2048>. Default<1024>: 1024

Host key already exists. Do you want to replace. [y/n] :y
FTOS(conf)#
```

Related Commands	[ip ssh server] – enables the SSH server. [show crypto] – displays the SSH host public keys.

debug ip ssh

Enables collecting SSH debug information.

S5000

Syntax

```
debug ip ssh {client | server}
```

To disable debugging, use the `no debug ip ssh {client | server}` command.

Parameters

client	Enter the keyword `client` to enable collecting debug information on the client.
server	Enter the keyword `server` to enable collecting debug information on the server.

Defaults Disabled on both client and server.

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Debug information includes details for key-exchange, authentication, and established session for each connection.

ip scp topdir

Identify a location for files used in secure copy transfer.

S5000

Syntax

```
ip scp topdir directory
```

To return to the default setting, use the `no ip scp topdir` command.

Parameters

directory	Enter a directory name.

Defaults The internal flash (`flash:`) is the default directory.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information To configure the switch as a SCP server, use the `ip ssh server` command.

Related Commands ip ssh server – enables the SSH and SCP server on the switch.

ip ssh authentication-retries

Configure the maximum number of attempts that should be used to authenticate a user.

S5000

Syntax `ip ssh authentication-retries 1-10`

Parameters

1-10	Enter the number of maximum retries to authenticate a user. The range is 1 to 10. The default is **3**.

Defaults **3**

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This command specifies the maximum number of attempts to authenticate a user on a SSH connection with the remote host for password authentication. SSH disconnects when the number of password failures exceeds authentication-retries.

ip ssh connection-rate-limit

Configure the maximum number of incoming SSH connections per minute.

S5000

Syntax `ip ssh connection-rate-limit 1-10`

Parameters

1-10	Enter the number of maximum number of incoming SSH connections allowed per minute. The range is 1 to 10 per minute. The default is **10 per minute**.

Defaults **10 per minute**

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

ip ssh hostbased-authentication

Enable hostbased-authentication for the SSHv2 server.

S5000

Syntax

`ip ssh hostbased-authentication enable`

To disable hostbased-authentication for SSHv2 server, use the `no ip ssh hostbased-authentication enable` command.

Parameters

enable	Enter the keyword `enable` to enable hostbased-authentication for SSHv2 server.

Defaults Disabled.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you enable this command, clients can login without a password prompt. This provides two levels of authentication:

- rhost-authentication is done with the file specified in the `ip ssh rhostfile` command.
- checking client host-keys is done with the file specified in the `ip ssh pub-key-file` command.

NOTE: Administrators must specify the two files (`rhosts` and `pub-key-file`) to configure host-based authentication.

Related Commands

ip ssh pub-key-file – public keys of trusted hosts from a file.

ip ssh rhostsfile – trusted hosts and users for rhost authentication.

ip ssh key-size

Configure the size of the server-generated RSA SSHv1 key.

S5000

Syntax

`ip ssh key-size *512-869*`

Parameters

512-869	Enter the key-size number for the server-generated RSA SSHv1 key. The range is 512 to 869. The default is **768**.

Defaults Key size **768**

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The server-generated key is used for SSHv1 key-exchange.

ip ssh password-authentication

Enable password authentication for the SSH server.

S5000

Syntax

```
ip ssh password-authentication enable
```

To disable password-authentication, use the `no ip ssh password-authentication enable` command.

Parameters

enable	Enter the keyword `enable` to enable password-authentication for the SSH server.

Defaults Enabled

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information With password authentication enabled, you can authenticate using the local, RADIUS, or TACACS+ password fallback order as configured.

ip ssh pub-key-file

Specify the file to be used for host-based authentication.

S5000

Syntax

```
ip ssh pub-key-file {WORD}
```

Parameters

WORD	Enter the file name for the host-based authentication.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command specifies the file to be used for the host-based authentication. The `creates/` file overwrites the `flash://ADMIN_DIR/ssh/knownhosts` file and deletes the user-specified file. Even though this is a global configuration command, it does not appear in the running configuration because this command needs to be run just once.

The file contains the OpenSSH-compatible public keys of the host for which host-based authentication is allowed. An example known host file format:

```
poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/
QQp8xYhzOxn07yh4VGPAoUfgKoieTHO9G4sNV+ui
+DWEc3cgYAcU5Lai1MU2ODrzhCwyDNp05tKBU3t
ReG1o8AxLi6+S4hyEMqHzkzBFNVqHzpQc
+Rs4p2urzV0F4pRKnaXdHf3Lk4D460HZRhhVrxqeNxPDpEn WIMPJi0ds=
ashwani@poclab4
```

NOTE: For `rhostfile` and `pub-key-file`, the administrator must FTP the file to the chassis.

Example

```
FTOS#conf
FTOS(conf)# ip ssh pub-key-file flash://knownhosts
FTOS(conf)#
```

Related Commands

show ip ssh client-pub-keys – displays the client-public keys used for the host-based authentication.

ip ssh rhostsfile

Specify the rhost file to be used for host-based authorization.

S5000

Syntax `ip ssh rhostsfile {WORD}`

Parameters

WORD	Enter the rhost file name for the host-based authentication.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#conf
FTOS(conf)# ip ssh rhostsfile flash://shosts
FTOS(conf)#
```

Usage Information

This command specifies the rhost file to be used for host-based authentication. This `creates/` file overwrites the `flash:/ADMIN_DIR/ssh/shosts` file and deletes the user-specified file. Even though this is a global configuration command, it does not appear in the running configuration because this command needs to be run just once.

This file contains hostnames and usernames, for which hosts and users, rhost-authentication can be allowed.

NOTE: For `rhostfile` and `pub-key-file`, the administrator must FTP the file to the switch.

ip ssh rsa-authentication (Config)

Enable RSA authentication for the SSHv2 server.

S5000

Syntax

`ip ssh rsa-authentication enable`

To disable RSA authentication, use the `no ip ssh rsa-authentication enable` command.

Parameters

enable	Enter the keyword `enable` to enable RSA authentication for the SSHv2 server.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Enabling RSA authentication allows the user to login without being prompted for a password. In addition, the OpenSSH compatible SSHv2 RSA public key must be added to the list of authorized keys (`ip ssh rsa-authentication my-authorized-keys device://filename` command).

Related Commands

ip ssh rsa-authentication (EXEC) – adds keys for RSA authentication.

ip ssh rsa-authentication (EXEC)

Add keys for the RSA authentication.

S5000

Syntax

```
ip ssh rsa-authentication {my-authorized-keys WORD}
```

To delete the authorized keys, use the `no ip ssh rsa-authentication {my-authorized-keys}` command.

Parameters

my-authorized-keys *WORD*	Enter the keywords `my-authorized-keys` followed by the file name of the RSA authorized-keys.

Defaults

none

Command Modes

EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you want to log in without being prompted for a password, log in through RSA authentication. To do that, you must first add the SSHv2 RSA public keys to the list of authorized keys. This command adds the specified RSA keys to the following file: `flash://ADMIN_DIR/ssh/authorized-keys-username` (where `username` is the user associated with this terminal).

NOTE: The `no` form of this command deletes the file `flash://ADMIN_DIR/ssh/authorized-keys-username` file.

Related Commands

show ip ssh rsa-authentication – displays the RSA authorized keys.

ip ssh rsa-authentication (Config) – enables RSA authentication.

ip ssh server

Configure an SSH server.

S5000

Syntax

NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

```
ip ssh server {enable | port port-number} [version {1 | 2}]
```

To disable SSH server functions, use the `no ip ssh server enable` command.

Parameters

enable	Enter the key word `enable` to start the SSH server.

port ***port-number***	(OPTIONAL) Enter the keyword `port` followed by the port number of the listening port of the SSH server. The range is 1 to 65535. The default is **22**.
[version {1 | 2}]	(OPTIONAL) Enter the keyword `version` followed by the SSH version 1 or 2 to specify only SSHv1 or SSHv2. **NOTE:** If you enable FIPS mode, you can only select version 2.

Defaults Default listening port is **22**.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This command enables the SSH server and begins listening on a port. If a port is not specified, listening is on SSH default port 22.

Example

```
FTOS# conf
FTOS(conf)# ip ssh server port 45
FTOS(conf)# ip ssh server enable
FTOS#
```

Related Commands show ip ssh – displays the ssh information.

show crypto

Display the public part of the SSH host-keys.

S5000

Syntax

NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

`show crypto key mypubkey {rsa | rsa1}`

Parameters

Key	Enter the keyword `key` to display the host public key.
mypubkey	Enter the keyword `mypubkey` to display the host public key.
rsa	Enter the keyword `rsa` to display the host SSHv2 RSA public key.
rsa1	Enter the keyword `rsa1` to display the host SSHv1 RSA public key. **NOTE:** If you enable FIPS mode, this parameter is not available.

Defaults none

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command is useful if the remote SSH client implements Strict Host Key Checking. You can copy the host key to your list of known hosts.

Example

```
FTOS#show crypto key mypubkey rsa
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtzkZME/
e8V8smnXR22EJGQhCMkEOkuisa+OILVoMYU1ZKGfj0W5BPCSvF/
x5ifqYFFwUzJNOcsJK7vjSsnmMhChF2YSvXlvTJ6h971FJAQlOsgd0ycpocsF
+DNLKfJnx7SAjhakFQMwG
g/g78ZkDT3Ydr8KKjfSI4Bg/WS8B740=

FTOS#show crypto key mypubkey rsa1
1024 35
131060015480873398953257515397249657850072206444294963674080935
6830889610203172266
798895675496676526500637962218977992760927852363883922305508181
9166009928132616408
664345774602219229518903992966334579117374224743155375050167692
9660273790601494434
050000015179864425629613385774919236081771341059533760063913083
FTOS#
```

Related Commands

crypto key generate – generates the SSH keys.

show ip ssh

Display information about established SSH sessions.

S5000

Syntax

NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

```
show ip ssh
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#sh ip ssh
SSH server                 : enabled.
SSH server version         : v1 and v2.
Password Authentication    : enabled.
Hostbased Authentication : disabled.
RSA Authentication         : disabled.
Vty  Encryption   HMAC       Remote IP
1    3des-cbc     hmac-md5   10.1.20.48
2    3des-cbc     hmac-md5   10.1.20.48
```

Related Commands

ip ssh server – configures an SSH server.

show ip ssh client-pub-keys – displays the client-public keys.

show ip ssh client-pub-keys

Display the client public keys used in host-based authentication.

S5000

Syntax

```
show ip ssh client-pub-keys
```

Defaults

none

Command Modes

EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command displays the contents of the `flash://ADMIN_DIRssh/knownhosts` file.

Example

```
FTOS#show ip ssh client-pub-keys

poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/
QQp8xYhzOxn07yh4VGPAoUfgKoieTHO9G4sNV+ui
+DWEc3cgYAcU5Lai1MU2ODrzhCwyDNp05tKBU3tReG1
o8AxLi6+S4hyEMqHzkzBFNVqHzpQc
+Rs4p2urzV0F4pRKnaXdHf3Lk4D460HZRhhVrxqeNxPDpEnWIMPJi0
ds= ashwani@poclab4

FTOS#
```

Related Commands

ip ssh pub-key-file – configures the file name for the host-based authentication.

show ip ssh rsa-authentication

Display the authorized-keys for the RSA authentication.

S5000

Syntax

```
show ip ssh rsa-authentication {my-authorized-keys}
```

Parameters

my-authorized-keys	Display the RSA authorized keys.

Defaults

none

Command Modes

EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command displays the contents of the `flash:/ADMIN_DIR/ssh/authorized-keys.username` file.

Example

```
FTOS#show ip ssh rsa-authentication my-authorized-keys
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAyB17l4gFp4r2DRHIvMc1VZd0Sg5GQxRV1y1
X1JOMeO6Nd0WuYyzrQMM
4qJAoBwtneOXfLBcHF3V2hcMIqaZN+CRCnw/
zCMlnCf0+qVTd1oofsea5r09kS0xTp0CNfHXZ3NuGCq9Ov33m9+U9tMwhS8vy8A
VxdH4x4km3c3t5Jvc=
freedom@poclab4

FTOS#
```

Related Commands

ip ssh rsa-authentication (Config) – configures the RSA authorized keys.

ssh

Open an SSH connection specifying the hostname, username, port number and version of the SSH client.

S5000

Syntax

NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

```
ssh {hostname | ipv4 address | ipv6 address} [-c encryption
cipher | -l username | -m HMAC algorithm | -p port-number | -v
{1 | 2}]
```

Parameters

hostname	(OPTIONAL) Enter the IP address or the hostname of the remote device.
ipv4 address	(OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.
ipv6-address prefix-length	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
-c *encryption cipher*	Enter the following encryption cipher. (For v2 clients only.): • `3des-cbc`: Force ssh to use 3des-cbc encryption cipher.
-l *username*	(OPTIONAL) Enter the keyword `-l` followed by the user name used in this SSH session. The default is the user name of the user associated with the terminal.

-m ***HMAC algorithm***	Enter one of the following HMAC algorithms to use. (For v2 clients only.): • `hmac-sha1`: Force ssh to use the hmac-sha1 HMAC algorithm. • `hmac-sha1-96`: Force ssh to use the hmac-sha1-96 HMAC algorithm. • `hmac-md5`: Force ssh to use the hmac-md5 HMAC algorithm. • `hmac-md5-96`: Force ssh to use the hmac-md5-96 HMAC algorithm.
-p ***port-number***	(OPTIONAL) Enter the keyword `-p` followed by the port number. The range is 1 to 65536. The default is **22**.
-v {1 | 2}	(OPTIONAL) Enter the keyword `-v` followed by the SSH version 1 or 2. The default is the version from the protocol negotiation.

Defaults As above.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information FTOS supports both inbound and outbound SSH sessions using IPv4 or IPv6 addressing. Inbound SSH supports accessing the system through the management interface as well as through a physical Layer 3 interface.

Example

```
FTOS#ssh 10.11.8.12 ?
-c         Encryption cipher to use (for v2 clients only)
-l         User name option
-m         HMAC algorithm to use (for v2 clients only)
-p         SSH server port option (default 22)
-v         SSH protocol version
<cr>

FTOS#ssh 10.11.8.12 -c ?
3des-cbc  Force ssh to use 3des-cbc encryption cipher

FTOS#ssh 10.11.8.12 -m ?
hmac-sha1    Force ssh to use hmac-sha1 HMAC algorithm
hmac-sha1-96 Force ssh to use hmac-sha1-96 HMAC algorithm
hmac-md5     Force ssh to use hmac-md5 HMAC algorithm
hmac-md5-96  Force ssh to use hmac-md5-96 HMAC algorithm
```

Secure DHCP Commands

DHCP as defined by RFC 2131 provides no authentication or security mechanisms. Secure DHCP is a suite of features that protects networks that use dynamic address allocation from spoofing and attacks.

clear ip dhcp snooping

Clear the DHCP binding table.

S5000

Syntax	`clear ip dhcp snooping binding`	
Defaults	none	
Command Modes	EXEC Privilege	
Command History	**Version 9.0(1.3)**	Introduced on the S5000.
Related Commands	show ip dhcp snooping – displays the contents of the DHCP binding table.	

ip dhcp relay

Enable Option 82.

S5000

Syntax	`ip dhcp relay information-option [trust-downstream]`	
Parameters	**trust-downstream**	Configure the system to trust Option 82 when it is received from the previous-hop router.
Defaults	Disabled.	
Command Modes	CONFIGURATION	
Command History	**Version 9.0(1.3)**	Introduced on the S5000.

ip dhcp snooping

Enable DHCP Snooping globally.

S5000

Syntax	`[no] ip dhcp snooping`
Defaults	Disabled.
Command Modes	CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When enabled, no learning takes place until you enable snooping on a VLAN. After disabling DHCP Snooping, the binding table is deleted and Option 82, IP Source Guard, and Dynamic ARP Inspection are disabled.

Related Commands

ip dhcp snooping vlan – enables DHCP Snooping on one or more VLANs.

ip dhcp snooping binding

Create a static entry in the DHCP binding table.

S5000

Syntax

```
[no] ip dhcp snooping binding mac address vlan-id vlan-id ip
ip-address interface type slot/port lease number
```

Parameters

mac *address*	Enter the keyword `mac` followed by the MAC address of the host to which the server is leasing the IP address.
vlan-id *vlan-id*	Enter the keywords `vlan-id` followed by the VLAN to which the host belongs. The range is 2 to 4094.
ip *ip-address*	Enter the keyword `ip` followed by the IP address that the server is leasing.
interface *type slot/port*	Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
slot/port	Enter the slot and port number of the interface.
lease *time*	Enter the keyword `lease` followed by the amount of time the IP address is leased. The range is 1 to 4294967295.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

Related Commands	show ip dhcp snooping – displays the contents of the DHCP binding table.

ip dhcp snooping database

Delay writing the binding table for a specified time.

S5000

Syntax `ip dhcp snooping database write-delay minutes`

Parameters	***minutes***	The range is 5 to 21600.

Defaults none

Command Modes CONFIGURATION

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

ip dhcp snooping database renew

Renew the binding table.

S5000

Syntax `ip dhcp snooping database renew`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

ip dhcp snooping trust

Configure an interface as trusted.

S5000

Syntax	`[no] ip dhcp snooping trust`
Defaults	Untrusted
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ip dhcp source-address-validation

Enable IP Source Guard.

S5000

Syntax	`[no] ip dhcp source-address-validation`
Defaults	Disabled.
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ip dhcp snooping vlan

Enable DHCP Snooping on one or more VLANs.

S5000

Syntax	`[no] ip dhcp snooping vlan` *`name`*
Parameters	***name*** Enter the name of a VLAN on which to enable DHCP Snooping.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Usage Information	When enabled, the system begins creating entries in the binding table for the specified VLAN(s). **NOTE:** Learning only happens if there is a trusted port in the VLAN.
Related Commands	ip dhcp snooping trust – configures an interface as trusted.

show ip dhcp snooping

Display the contents of the DHCP binding table.

S5000

Syntax	`show ip dhcp snooping binding`
Defaults	none
Command Modes	• EXEC • EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	clear ip dhcp snooping – clears the contents of the DHCP binding table.

49

Service Provider Bridging

Service provider bridging is composed of virtual local area network (VLAN) Stacking, Layer 2 Protocol Tunneling, and Provider Backbone Bridging as described in the *FTOS Configuration Guide Service Provider Bridging* chapter.

This chapter includes command line information (CLI) for the Dell Networking operating software (FTOS) Layer 2 Protocol Tunneling (L2PT). L2PT enables protocols to tunnel through an 802.1q tunnel.

FTOS supports L2PT on the S5000 switch.

For more information, refer to VLAN Stacking, Spanning Tree Protocol (STP), and GARP VLAN Registration (GVRP).

Important Points to Remember

- L2PT is enabled at the interface VLAN-Stack VLAN level. For more information about Stackable VLAN (VLAN-Stacking) commands, refer to VLAN Stacking.
- The default behavior is to disable protocol packet tunneling through the 802.1q tunnel.
- Rate-limiting is required to protect against bridge protocol data units (BPDU) attacks.
- A port channel (including through link aggregation control protocol [LACP]) can be configured as a VLAN-Stack access or trunk port.
- Address resolution protocol (ARP) packets work as expected across the tunnel.
- Far-end failure detection (FEFD) works the same as with Layer 2 links.
- Protocols that use Multicast MAC addresses (for example, open shortest path first [OSPF]) work as expected and carry over to the other end of the VLAN-Stack VLAN.

debug protocol-tunnel

Enable debugging to ensure incoming packets are received and rewritten to a new MAC address.

S5000

Syntax

`debug protocol-tunnel {interface-type slot/port in | out | both} [vlan vlan-id] [count value]}`

To disable debugging, use the `no debug protocol-tunnel interface {in | out | both} [vlan vlan-id] [count value]` command.

Parameters

interface-type slot/port	Enter one of the following interfaces and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below.

- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

in | out | both	Enter the keyword `in`, `out`, or `both` to debug incoming interfaces, outgoing interfaces, or both incoming and outgoing interfaces.
vlan *vlan-id*	Enter the keyword `vlan` followed by the VLAN id number from 1 to 4094.
count *value*	Enter the keyword `count` followed by the number of debug outputs. The range is 1 to 100.

Defaults Debug disabled.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

protocol-tunnel

Enable protocol tunneling on a stacked (Q-in-Q) VLAN for specified protocol packets.

S5000

Syntax `protocol-tunnel {stp}`

To disable protocol tunneling for a Layer 2 protocol, use the `no protocol-tunnel` command.

Parameters

stp	Enter the keyword `stp` to enable protocol tunneling on a spanning tree, including STP, MSTP, RSTP, and PVST.

Defaults none

Command Modes CONF-IF-VLAN

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#conf
FTOS(conf)#interface vlan 2
FTOS(conf-if-vl-2)#vlan-stack compatible
FTOS(conf-if-vl-2)#member Te1/2-3
FTOS(conf-if-vl-2)#protocol-tunnel stp
FTOS(conf-if-vl-2)#protocol-tunnel enable
```

Related Command	show protocol-tunnel – displays tunneling information for all VLANs.

protocol-tunnel destination-mac

Overwrite the BPDU destination MAC address with a specific value.

S5000

Syntax `protocol-tunnel destination-mac xstp address`

Parameters

stp	Change the default destination MAC address used for L2PT to another value.

Defaults The default destination MAC is 01:01:e8:00:00:00.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information When you enable VLAN-Stacking, no protocol packets are tunneled.

Related Command show protocol-tunnel – displays tunneling information for all VLANs.

protocol-tunnel enable

Enable protocol tunneling globally on the system.

S5000

Syntax `protocol-tunnel enable`

To disable protocol tunneling, use the `no protocol-tunnel enable` command.

Defaults Disabled.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information FTOS must have the default CAM profile with the default microcode before you enable L2PT.

protocol-tunnel rate-limit

Enable traffic rate limiting per box.

S5000

Syntax	`protocol-tunnel rate-limit` *`rate`* To reset the rate limit to the default, use the `no protocol-tunnel rate-limit` *`rate`* command.
Parameters	*rate* — Enter the rate in frames per second. The range is 75 to 3000. The default is **75**.
Defaults	**75** frames per second.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

Example

```
FTOS#
FTOS#conf
FTOS(conf)#protocol-tunnel rate-limit 1000
FTOS(conf)#
```

Related Commands

show protocol-tunnel – displays tunneling information for all VLANs.

show running-config – displays the current configuration.

show protocol-tunnel

Display protocol tunnel information for all or a specified VLAN-Stack VLAN.

S5000

Syntax	`show protocol-tunnel [vlan` *`vlan-id`*`]`
Parameters	**vlan** ***vlan-id*** — (OPTIONAL) Enter the keyword `vlan` followed by the VLAN ID to display information for the one VLAN. The range is 1 to 4094.
Defaults	none
Command Modes	EXEC
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

Example

```
FTOS#show protocol-tunnel
System Rate-Limit: 75 frames/second
VLAN  Protocols   Interface
```

```
1000  STP,PVST    Te 5/7,Te 5/6
1001  LLDP,GVRP   Te 5/7,Te 5/6
1002  MMRP,MVRP   Te 5/7,Te 5/6
1003  LACP,DOT1X  Te 5/7,Te 5/6
1004  OAM,PAUSE   Te 5/7,Te 5/6
1005  E-LMI       Te 5/7,Te 5/6
```

Example (Specific VLAN)

```
FTOS#show protocol-tunnel vlan 2
System Rate-Limit: 1000 Frames/second
Interface  Vlan  Protocol(s)
Te1/2      2     STP, PVST
FTOS#
```

Related Commands

show running-config – displays the current configuration.

50

sFlow

FTOS supports sFlow commands on the S5000 switch.

FTOS sFlow monitoring system includes an sFlow Agent and an sFlow Collector.

- The sFlow Agent combines the flow samples and interface counters into sFlow datagrams and forwards them to the sFlow Collector.
- The sFlow Collector analyzes the sFlow Datagrams received from the different devices and produces a network-wide view of traffic flows.

Important Point to Remember

- Dell Networking recommends that the sFlow Collector be connected to the Dell Networking chassis through the interface rather than the Management Ethernet interface.
- FTOS exports all sFlow packets to the sFlow Collector. A small sampling rate can equate to a large number of exported packets. A backoff mechanism is automatically applied to reduce this amount. Some sampled packets may be dropped when the exported packet rate is high and the backoff mechanism is about to or is starting to take effect. The dropEvent counter, in the sFlow packet, is always zero.
- sFlow sampling is done on a per-port basis.
- Community list and local preference fields are not filled up in the extended gateway element in the sFlow datagram.
- The 802.1P source priority field is not filled up in the extended switch element in the sFlow datagram.
- Only Destination and Destination Peer AS numbers are packed in the dst-as-path field in the extended gateway element.
- If the packet being sampled is redirected using policy-based routing (PBR), the sFlow datagram may contain incorrect extended gateway/router information.
- sFlow does not support packing extended information for IPv6 packets. Only the first 128 bytes of the IPv6 packet is shipped in the datagram.
- The source virtual local area network (VLAN) field in the extended switch element is not packed in case of a routed packet.
- The destination VLAN field in the extended switch element is not packed in case of a multicast packet.
- The maximum number of packets that can be sampled and processed per second is:
  - 7500 packets when no extended information packing is enabled.
  - 7500 packets when only extended-switch information packing is enabled (refer to sflow extended-switch enable).
  - 1600 packets when extended-router and/or extended-gateway information packing is enabled (refer to sflow extended-gateway enable)

sflow collector

Configure a collector device to which sFlow datagrams are forwarded.

S5000

Syntax

`sflow collector {`*`ipv4-address`*` | `*`ipv6-address`*`} agent-addr {`*`ipv4-address`*` | `*`ipv6-address`*`} [`*`number`*` [max-datagram-size `*`number`*`]] | [max-datagram-size `*`number`*`]`

To delete a configured collector, use the `no sflow collector {`*`ipv4-address`*` | `*`ipv6-address`*`} agent-addr {`*`ipv4-address`*` | `*`ipv6-address`*`} [`*`number`*` [max-datagram-size `*`number`*`]] | [max-datagram-size `*`number`*`]` command.

Parameters

sflow collector *ipv4-address* | *ipv6-address*	Enter the IPv4 (A.B.C.D) or IPv6 address (X:X:X:X::X) of the sFlow collector device.
agent-addr *ipv4-address* | *ipv6-address*	Enter the IPv4 (A.B.C.D) or IPv6 address (X:X:X:X::X) of the sFlow agent in the router.
number	(OPTIONAL) Enter the user datagram protocol (UDP) port number. The range is 0 to 65535. The default is 6343.
max-datagram-size *number*	(OPTIONAL) Enter the keyword max-datagram-size followed by the size number in bytes. The range is 400 to 1500. The default is **1400**.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can configure up to two sFlow collectors (IPv4 or IPv6). If two collectors are configured, traffic samples are sent to both.

The sFlow agent address is carried in a field in SFlow packets and is used by the collector to identify the sFlow agent.

IPv6 sFlow collectors and agents are supported on the S5000 switch.

As part of the sFlow-MIB, if the SNMP request originates from a configured collector, FTOS returns the corresponding configured agent IP in the MIB requests. FTOS checks to ensure that two entries are not configured for the same collector IP with a different agent IP. Should that happen, FTOS generates the following error: `%Error: Different agent-addr attempted for an existing collector.`

sflow enable (Global)

Enable sFlow globally.

S5000

Syntax

`sflow enable`

To disable sFlow, use the `no sflow enable` command.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

sFlow is disabled by default. In addition to this command, sFlow needs to be enable on individual interfaces where sFlow sampling is desired.

Related Commands

sflow enable (Interface) – enables sFlow on Interfaces.

sflow enable (Interface)

Enable sFlow on Interfaces.

S5000

Syntax

`sflow enable`

To disable sFlow, use the `no sflow enable` command.

Defaults

Disabled.

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you enable sFlow on an interface, flow sampling is done on any traffic going out of the interface.

NOTE: After a physical port is a member of a LAG, it inherits the sFlow configuration from the LAG port.

Related Commands

sflow enable (Global) – turns sFlow on globally.

sflow extended-switch enable

Enable packing information on a switch only.

S5000

Syntax	`sflow extended-switch enable` To disable packing information, use the `no sflow extended-switch [enable]` command.
Parameters	**enable** — Enter the keyword `enable` to enable global extended information.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** — Introduced on the S5000.
Related Commands	sflow extended-gateway enable – enables packing information on an extended gateway. sflow extended-router enable – enables packing information on a router. show sflow – displays the sFlow configuration.

sflow polling-interval (Global)

Set the sFlow polling interval at a global level.

S5000

Syntax	`sflow polling-interval interval value` To return to the default, use the `no sflow polling-interval interval` command.
Parameters	***interval value*** — Enter the interval value in seconds. The range is 15 to 86400 seconds. The default is **20 seconds**.
Defaults	**20 seconds**
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** — Introduced on the S5000.
Usage Information	The polling interval for an interface is the maximum number of seconds between successive samples of counters to be sent to the collector. This command changes the global default counter polling (20 seconds) interval. You can configure an interface to use a different polling interval.

Related Commands	sflow polling-interval (Interface) – sets the polling interval for an interface.

sflow polling-interval (Interface)

Set the sFlow polling interval at an interface (overrides the global-level setting.)

S5000

Syntax

`sflow polling-interval interval value`

To return to the default, use the `no sflow polling-interval interval` command.

Parameters

interval value	Enter the interval value in seconds. The range is 15 to 86400 seconds. The default is **the global counter polling interval**.

Defaults

The same value as the current global default counter polling interval.

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command sets the counter polling interval for an interface.

Related Commands

sflow polling-interval (Global) – globally sets the polling interval.

sflow sample-rate (Global)

Change the global default sampling rate.

S5000

Syntax

`sflow sample-rate value`

To return to the default sampling rate, use the `no sflow sample-rate` command.

Parameters

value	Enter the sampling rate value. The range is 256 to 8388608 packets.

Defaults

32768 packets

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	Sample-rate is the average number of packets skipped before the sample is taken. This command changes the global default sampling rate. You can configure an interface to use a different sampling rate than the global sampling rate. If the value entered is not a correct power of 2, the command generates an error message with the previous and next power of 2 value. Select one of these two packet numbers and re-enter the command.
Related Commands	sflow sample-rate (Interface) – changes the Interface sampling rate.

sflow sample-rate (Interface)

Change the Interface default sampling rate.

S5000

Syntax	`sflow sample-rate value` To return to the default sampling rate, use the `no sflow sample-rate` command.
Parameters	***value*** — Enter the sampling rate value. The range is 256 to 8388608 packets.
Defaults	The Global default sampling.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** — Introduced on the S5000.
Usage Information	This command changes the sampling rate for an Interface. By default, the sampling rate of an interface is set to the same value as the current global default sampling rate. If the value entered is not a correct power of 2, the command generates an error message with the previous and next power-of-2 value. Select one of these two number and re-enter the command.
Related Commands	sflow sample-rate (Global) – changes the sampling rate globally.

show sflow

Display the current sFlow configuration.

S5000

Syntax	`show sflow [interface type slot/port]`

Parameters

interface ***type slot/port***	(OPTIONAL) Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The dropEvent counter (sFlow samples dropped due to sub-sampling) shown in the Example below always displays a value of zero.

Example

```
FTOS#show sflow
sFlow services are enabled
Global default sampling rate: 32768
Global default counter polling interval: 20
1 collectors configured
Collector IP addr: 133.33.33.53, Agent IP addr: 133.33.33.116,
UDP port: 6343
0 UDP packets exported
0 UDP packets dropped
165 sFlow samples collected
```

0 sFlow samples dropped due to sub-sampling

```
Stack-unit 1 Port set 0 H/W sampling rate 8192
  Te 1/16: configured rate 8192, actual rate 8192, sub-
sampling rate 1
  Te 1/17: configured rate 16384, actual rate 16384, sub-
sampling rate 2
Stack-unit 3 Port set 1 H/W sampling rate 16384
  Te 3/40: configured rate 16384, actual rate 16384, sub-
sampling rate 1
FTOS#
```

show sflow stack-unit

Display the sFlow information on a stack-unit.

S5000

Syntax `show sflow stack—unit {unit-number}`

Parameters

unit-number	(OPTIONAL) Enter the `stack-unit` keyword followed by the unit number. The range is 0 to 11.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on S5000.

Usage Information The dropEvent counter (sFlow samples dropped due to sub-sampling) shown in the Example below always displays a value of zero.

Example

```
FTOS#show sflow stack-unit 0
Stack-Unit 0
  Samples rcvd from h/w             :0
  Total UDP packets exported        :0
  UDP packets exported              :0
  UDP packets dropped               :0
FTOS#
```

51

Simple Network Management Protocol (SNMP) and Syslog

This chapter contains commands to configure and monitor the simple network management protocol (SNMP) v1/v2/v3 and Syslog. Both features are supported on the S5000 switch.

The chapter contains the following sections:

- SNMP Commands
- Syslog Commands

SNMP Commands

The following SNMP commands are available in the Dell Networking operating software (FTOS).

The simple network management protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements. FTOS supports SNMP versions 1, 2c, and 3, supporting both read-only and read-write modes. FTOS sends SNMP traps, which are messages informing an SNMP management system about the network. FTOS supports up to 16 SNMP trap receivers.

Important Points to Remember

- Typically, 5-second timeout and 3-second retry values on an SNMP server are sufficient for both LAN and WAN applications. If you experience a timeout with these values, the recommended best practice on Dell Networking switches (to accommodate their high port density) is to increase the timeout and retry values on your SNMP server to the following:
    - SNMP Timeout—greater than 3 seconds.
    - SNMP Retry count—greater than 2 seconds.
- SNMP v3 informs are not currently supported with IPv6 addresses.
- If you are using access control lists (ACLs) in an SNMP v3 configuration, group ACL overrides user ACL if the user is part of that group.
- SNMP operations are not supported on a virtual local area network (VLAN).

show snmp

Display the status of SNMP network elements.

S5000

Syntax

```
show snmp
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show snmp
      62112 SNMP packets input
          0 Bad SNMP version errors
          0 Unknown community name
          0 Illegal operation for community name supplied
          0 Encoding errors
    2167317 Number of requested variables
          0 Number of altered variables
      53654 Get-request PDUs
       3324 Get-next PDUs
          0 Set-request PDUs
      62112 SNMP packets output
          0 Too big errors (Maximum packet size 1500)
          0 No such name errors
          0 Bad values errors
          0 General errors
      62112 Response PDUs
          0 Trap PDUs
```

Related Commands

snmp-server community – enables the SNMP and set community string.

show snmp engineID

Display the identification of the local SNMP engine and all remote engines that are configured on the router.

S5000

Syntax

```
show snmp engineID
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show snmp engineID
Local SNMP engineID: 0000178B02000001E80214A8
Remote Engine ID       IP-addr       Port
80001F88043132333435   172.31.1.3    5009
80001F88043938373635   172.31.1.3    5008

FTOS#
```

Related Commands

snmp-server engineID – configures local and remote SNMP engines on the router.

show snmp group

Display the group name, security model, status, and storage type of each group.

S5000

Syntax

`show snmp group`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following Example displays a group named *ngroup*. The *ngroup* has a security model of version 3 (v3) with authentication (`auth`), the read and notify name is *nview* with no write view name specified, and finally the row status is active.

Example

```
FTOS#show snmp group

groupname: v1v2creadg           security model: v1
readview : v1v2cdefault        writeview: no write view specified
notifyview: v1v2cdefault       context: no context specified
row status: active
groupname: v1v2creadg           security model: v2c
readview : v1v2cdefault        writeview: no write view specified
notifyview: v1v2cdefault       context: no context specified
row status: active
groupname: v1v2cwriteg          security model: v1
readview : v1v2cdefault        writeview: v1v2cdefault
notifyview: v1v2cdefault       context: no context specified
row status: active
groupname: v1v2cwriteg           security model: v2c
readview : v1v2cdefault        writeview: v1v2cdefault
notifyview: v1v2cdefault       context: no context specified
```

row status: active

Related Commands	snmp-server group – configures an SNMP server group.

show snmp user

Display the information configured on each SNMP user name.

S5000

Syntax

```
show snmp user
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show snmp user
User name: v1v2creadu
Engine ID: 0000178B02005CF9DDEF0200
storage-type: nonvolatile        active
Authentication Protocol: None
Privacy Protocol: None

User name: v1v2cwriteu
Engine ID: 0000178B02005CF9DDEF0200
storage-type: nonvolatile        active
Authentication Protocol: None
Privacy Protocol: None
```

snmp ifmib ifalias long

Display the entire description string through the interface MIB, which would be truncated otherwise to 63 characters.

S5000

Syntax

```
snmp ifmib ifalias long
```

Defaults Interface description truncated beyond 63 characters.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
!----command run on host connected to switch:------!
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i
alias | more
IF-MIB::ifAlias.134530304 = STRING: This is a port connected
to Router2. This is a
port connected to
IF-MIB::ifAlias.134792448 = STRING:

!----command run on Dell switch:-----------!
FTOS#snmp ifmib ifalias long

!----command run on server connected to switch:------!
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i
alias | more
IF-MIB::ifAlias.134530304 = STRING: This is a port connected
to Router2. This is a
port connected to Router2. This is a port connected to
Router2. This is a port
connected to Router2. This is a port connected to Router2.
IF-MIB::ifAlias.134792448 = STRING:
```

snmp-server community

Configure a new community string access for SNMPv1 v2 and v3.

S5000

Syntax

`snmp-server community` *`community-name`* `{ro | rw} [ipv6` *`ipv6-access-list-name`* `[ipv6` *`ipv6-access-list-name`* `|` *`access-list-name`* `| security-name` *`name`*`] | security-name` *`name`* `[ipv6` *`ipv6-access-list-name`* `|` *`access-list-name`* `| security-name` *`name`*`] |` *`access-list-name`* `[ipv6` *`ipv6-access-list-name`* `|` *`access-list-name`* `| security-name` *`name`*`]]]`

To remove access to a community, use the `no snmp-server community` *`community-string`* `{ro | rw} [security-name` *`name`* `[`*`access-list-name`* `| ipv6` *`access-list-name`* `|` *`access-list-name`* `ipv6` *`access-list-name`*`]]` command.

Parameters

community-name	Enter a text string (up to 20 characters long) to act as a password for SNMP.
ro	Enter the keyword `ro` to specify read-only permission.
rw	Enter the keyword `rw` to specify read-write permission.
ipv6 *access-list-name*	(Optional) Enter the keyword `ipv6` followed by a an IPv6 ACL name (a string up to 16 characters long).
security-name *name*	(Optional) Enter the keywords `security-name` followed by the security name as defined by the community MIB.
access-list-name	(Optional) Enter a standard IPv4 access list name (a string up to 16 characters long).

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on theS5000.

Usage Information

The Example below configures a community named *public* that is mapped to the security named *guestuser* with Read Only (`ro`) permissions.

The `security-name` parameter maps the community string to an SNMPv3 user/security name as defined by the community MIB.

If a community string is configured without a `security-name` (for example, `snmp-server community public ro`), the community is mapped to a default security-name/group:

- `v1v2creadu / v1v2creadg` — maps to a community with `ro` (read-only) permissions.
- `v1v2cwriteu/ v1v2cwriteg` — maps to a community with `rw` (read-write) permissions.

This command is indexed by the `community-name` parameter.

If you do not configure the `snmp-server community` command, you cannot query SNMP data. Only Standard IPv4 ACL and IPv6 ACL is supported in the optional `access-list-name`.

The command options `ipv6`, `security-name`, and `access-list-name` are recursive. In other words, each option can, in turn, accept any of the three options as a sub-option, and each of those sub-options can accept any of the three sub-options as a sub-option, and so forth. The second Example shows the creation of a standard IPv4 ACL called *snmp-ro-acl* and then assigning it to the SNMP community *guest*.

NOTE: For IPv6 ACLs, only IPv6 and UDP types are valid for SNMP; TCP and ICMP rules are not valid for SNMP. In IPv6 ACLs, port rules are not valid for SNMP.

Example

```
FTOS#config
FTOS(conf)# snmp-server community public ro
FTOS(conf)# snmp-server community guest ro security-name
guestuser
FTOS(conf)#
```

Example

```
FTOS(conf)# ip access-list standard snmp-ro-acl
FTOS(config-std-nacl)#seq 5 permit host 10.10.10.224
FTOS(config-std-nacl)#seq 10 deny any count
!

FTOS(conf)#snmp-server community guest ro snmp-ro-acl
FTOS(conf)#
```

Related Commands

ip access-list standard – names (or selects) a standard access list to filter based on IP address.

ipv6 access-list – configures an access list based on IPv6 addresses or protocols.

show running-config snmp – displays the current SNMP configuration and defaults.

snmp-server contact

Configure contact information for troubleshooting this SNMP node.

S5000

Syntax

`snmp-server contact text`

To delete the SNMP server contact information, use the `no snmp-server contact` command.

Parameters

text	Enter an alphanumeric text string, up to 55 characters long.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

snmp-server enable traps

Enable SNMP traps.

S5000

Syntax

`snmp-server enable traps [notification-type] [notification-option]`

To disable traps, use the `no snmp-server enable traps [notification-type] [notification-option]` command.

Parameters

notification-type	Enter the type of notification from the list below: • `bgp`—Notification of changes in the BGP process. • `ecfm`—Notification of changes to ECFM. • `envmon`—For Dell Networking, device notifications when an environmental threshold is exceeded. • `isis`—Notification of intermediate service traps. • `lacp`—Notification of changes. • `snmp`—Notification of RFC 1157 traps. • `stp`—Notification of a state change in the spanning tree protocol (RFC 1493). • `vlt`—Notification of virtual link trunking. • `vrrp`—Notification of a state change in a VRRP group. • `xstp`—Notification of a state change in MSTP (802.1s), RSTP (802.1w), and PVST+.

notification-option	For the `envmon` notification-type, enter one of the following optional parameters: • `cam-utilization` • `fan` • `supply` • `temperature` For the `snmp` notification-type, enter one of the following optional parameters: • `authentication` • `coldstart` • `linkdown` • `linkup`

Defaults Not enabled.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

FTOS supports up to 16 SNMP trap receivers.

For the `cam-utilization` notification option, the system generates syslogs and SNMP traps when the L3 host table or route table utilization goes above the threshold.

If you do not configure this command, no traps controlled by this command are sent. If you do not specify a `notification-type` and `notification-option`, all traps are enabled.

Related Commands

snmp-server community – enables SNMP and sets the community string.

snmp-server engineID

Configure the name for both the local and remote SNMP engines on the router.

S5000

Syntax

`snmp-server engineID [local *engineID*] [remote *ip-address* udp-port *port-number* *engineID*]`

To return to the default, use the `no snmp-server engineID [local *engineID*] [remote *ip-address* udp-port *port-number* *engineID*]` command.

Parameters

local *engineID*	Enter the keyword `local` followed by the engine ID number that identifies the copy of the SNMP on the local device. Format (as specified in RFC 3411): 12 octets.

- The first four octets are set to the private enterprise number.
- The remaining eight octets are the MAC address of the chassis.

remote *ip-address*	Enter the keyword `remote` followed by the IP address that identifies the copy of the SNMP on the remote device.
udp-port *port-number engineID*	Enter the keywords `udp-port` followed by the user datagram protocol (UDP) port number on the remote device. The range is 0 to 65535. The default is **162**.

Defaults As above.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Changing the value of the SNMP Engine ID has important side effects. A user's password (entered on the command line) is converted to an message digest algorithm (MD5) or secure hash algorithm (SHA) security digest. This digest is based on both the password and the local Engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of the Engine ID changes, the security digests of SNMPv3 users will be invalid and the users will have to be reconfigured.

For the remote Engine ID, the host IP and UDP port are the indexes to the command that are matched to either overwrite or remove the configuration.

Related Commands

show snmp engineID – displays the SNMP engine and all the remote engines that are configured on the router.

show running-config snmp – displays the SNMP running configuration.

snmp-server group

Configure a new SNMP group or a table that maps SNMP users to SNMP views.

S5000

Syntax

```
snmp-server group [group_name {1 | 2c | 3 {auth | noauth |
priv}}] [read name] [write name] [notify name] [access access-
list-name | ipv6 access-list-name | access-list-name ipv6
access-list-name]]
```

To remove a specified group, use the `no snmp-server group [group_name {v1 | v2c | v3 {auth | noauth | priv}}] [read name] [write name] [notify name] [access access-list-name | ipv6 access-list-name | access-list-name ipv6 access-list-name]]` command.

Parameters

group_name	Enter a text string (up to 20 characters long) as the name of the group. The following groups are created for mapping to read/write community/security-names (defaults):

	• `v1v2creadg` — maps to a community/security-name with `ro` permissions. • `1v2cwriteg` — maps to a community/security-name `rw` permissions.
1 | 2c | 3	(OPTIONAL) Enter the security model version number (`1`, `2c`, or `3`): • `1` is the least secure version. • `3` is the most secure of the security modes. • `2c` allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed. The default is **1**.
auth	(OPTIONAL) Enter the keyword `auth` to specify authentication of a packet without encryption.
noauth	(OPTIONAL) Enter the keyword `noauth` to specify no authentication of a packet.
priv	(OPTIONAL) Enter the keyword `priv` to specify both authentication and then scrambling of the packet.
read ***name***	(OPTIONAL) Enter the keyword `read` followed by a name (a string of up to 20 characters long) as the read view name. The default is **GlobalView** and is assumed to be every object belonging to the internet (1.3.6.1) OID space.
write ***name***	(OPTIONAL) Enter the keyword `write` followed by a name (a string of up to 20 characters long) as the write view name.
notify ***name***	(OPTIONAL) Enter the keyword `notify` followed by a name (a string of up to 20 characters long) as the notify view name.
access ***access-list-name***	(Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).
ipv6 ***access-list-name***	(Optional) Enter the keyword `ipv6` followed by the IPv6 access list name (a string up to 16 characters long).
access-list-name **ipv6** ***access-list-name***	(Optional) Enter both an IPv4 and IPv6 access list name.

Defaults As above.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The following Example specifies the group named *harig* as a version 3 user requiring both authentication and encryption and read access limited to the read named *rview*.

NOTE: The number of configurable groups is limited to 16 groups.

Example	`FTOS#conf`
	`FTOS(conf)# snmp-server group harig 3 priv read rview`
	`FTOS#`

Related Commands	show snmp group – displays the group name, security model, view status, and storage type of each group. show running-config – displays the SNMP running configuration.

snmp-server host

Configure the recipient of an SNMP trap operation.

S5000

Syntax

```
snmp-server host ip-address | ipv6-address [traps | informs]
[version 1 | 2c | 3] [auth | no auth | priv] [community-string]
[udp-port port-number] [notification-type]
```

To remove the SNMP host, use the `no snmp-server host ip-address [traps | informs] [version 1 | 2c | 3] [auth | noauth | priv] [community-string] [udp-port number] [notification-type]` command.

Parameters

ip-address	Enter the keyword `host` followed by the IP address of the host (configurable hosts is limited to 16).
ipv6-address	Enter the keyword host followed by the IPv6 address of the host in the x:x:x:x::x format. **NOTE:** The :: notation specifies successive hexadecimal fields of zero.
traps	(OPTIONAL) Enter the keyword `traps` to send trap notifications to the specified host. The default is **traps**.
informs	(OPTIONAL) Enter the keyword `informs` to send inform notifications to the specified host. The default is **traps**.
version 1 | 2c | 3	(OPTIONAL) Enter the keyword version to specify the security model followed by the security model version number `1`, `2c`, or `3`: • Version `1` is the least secure version. • Version `3` is the most secure of the security modes. • Version `2c` allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed. The default is version **1**.
auth	(OPTIONAL) Enter the keyword `auth` to specify authentication of a packet without encryption.

noauth	(OPTIONAL) Enter the keyword `noauth` to specify no authentication of a packet.
priv	(OPTIONAL) Enter the keyword `priv` to specify both authentication and then scrambling of the packet.
community-string	Enter a text string (up to 20 characters long) as the name of the SNMP community. **NOTE:** For version 1 and version 2c security models, this string represents the name of the SNMP community. The string can be set using this command; however, Dell Networking recommends setting the community string using the `snmp-server community` command before executing this command. For version 3 security model, this string is the USM user security name.
udp-port ***port-number***	(OPTIONAL) Enter the keywords `udp-port` followed by the port number of the remote host to use. The range is 0 to 65535. The default is **162**.
notification-type	(OPTIONAL) Enter one of the following keywords for the type of trap to be sent to the host: • `bgp` - BGP state change. • `envmon` - Environment monitor trap. • `snmp` - SNMP notification (RFC 1157). • `stp` - Spanning tree protocol notification (RFC 1493). • `vrrp` - State change in a VRRP group. • `xstp` - State change in MSTP (802.1s), RSTP (802.1w), and PVST+. The default is all trap types are sent to host.

Defaults As above.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

In order to configure the router to send SNMP notifications, you must enter at least `one snmp-server host` command. If you enter the command with no keywords, all trap types are enabled for the host. If you do not enter an `snmp-server host` command, no notifications are sent.

In order to enable multiple hosts, you must issue a separate `snmp-server host` command for each host. You can specify multiple notification types in the command for each host.

When multiple `snmp-server host` commands are given for the same host and type of notification (trap or inform), each succeeding command overwrites the previous command. Only the last `snmp-server host` command will be in effect. For example, if you enter an `snmp-server host inform` command for a host and then enter another `snmp-server host inform` command for the same host, the second command replaces the first command.

The `snmp-server host` command is used in conjunction with the `snmp-server enable` command. Use the `snmp-server enable` command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one `snmp-server enable` command and the `snmp-server host` command for that host must be enabled.

NOTE: For v1 / v2c trap configuration, if the community-string is not defined using the `snmp-server community` command prior to using this command, the default form of the `snmp-server community` command automatically is configured with the community-name the same as specified in the `snmp-server host` command.

Configuring Informs

To send an inform, use the following steps:

1. Configure a remote engine ID.
2. Configure a remote user.
3. Configure a group for this user with access rights.
4. Enable traps.
5. Configure a host to receive informs.

Related Commands

snmp-server enable traps – enables SNMP traps.

snmp-server community – configures a new community SNMPv1 or SNMPv2c.

snmp-server location

Configure the location of the SNMP server.

S5000

Syntax

`snmp-server location text`

To delete the SNMP location, use the `no snmp-server location` command.

Parameters

text	Enter an alpha-numeric text string, up to 55 characters long.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

snmp-server packetsize

Set the largest SNMP packet size permitted. Wen the SNMP server is receiving a request or generating a reply, use the `snmp-server packetsize global configuration` command.

S5000

Syntax `snmp-server packetsize` *`byte-count`*

Parameters

byte-count	Enter one of the following values 8, 16, 24 or 32. Packet sizes are 8000 bytes, 16000 bytes, 32000 bytes, and 64000 bytes.

Defaults 8

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

snmp-server trap-source

Configure a specific interface as the source for SNMP traffic.

S5000

Syntax `snmp-server trap-source` *`interface-type slot/port`*

To disable sending traps out a specific interface, use the `no snmp trap-source` command.

Parameters

interface-type slot/port

Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below.

- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.
- For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
- For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults The IP address assigned to the management interface is the default.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

For this `snmp-server trap-source` command to be enabled, you must configure an IP address on the interface and enable the interface configured as an SNMP trap source.

Related Commands

snmp-server community – sets the community string.

snmp-server user

Configure a new user to an SNMP group.

S5000

Syntax

```
snmp-server user name {group_name remote ip-address udp-port
port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-
password] [priv des56 priv password] [access access-list-name |
ipv6 access-list-name | access-list-name ipv6 access-list-name]
```

To remove a user from the SNMP group, use the `no snmp-server user name {group_name remote ip-address udp-port port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-password] [priv des56 priv password] [access access-list-name | ipv6 access-list-name | access-list-name ipv6 access-list-name]` command.

Parameters

name	Enter the name of the user (not to exceed 20 characters), on the host that connects to the agent.
group_name	Enter a text string (up to 20 characters long) as the name of the group. The following groups are created for mapping to read/write community/security-names (defaults): • `v1v2creadu` — maps to a community with `ro` permissions. • `1v2cwriteu` — maps to a community `rw` permissions.
remote *ip-address*	Enter the keywords `udp-port` followed by the user datagram protocol (UDP) port number on the remote device. The range is 0 to 65535. The default is **162**.
udp-port *port-number*	Enter the keywords `udp-port` followed by the UDP (User Datagram Protocol) port number on the remote device. The range is 0 to 65535. The default is **162**.
1 | 2c | 3	(OPTIONAL) Enter the security model version number (`1`, `2c`, or `3`): • `1` is the least secure version. • `3` is the most secure of the security modes. • `2c` allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.

	The default is **1**.
encrypted	(OPTIONAL) Enter the keyword `encrypted` to specify the password appear in encrypted format (a series of digits, masking the true characters of the string).
auth	(OPTIONAL) Enter the keyword `auth` to specify authentication of a packet without encryption.
md5 | sha	(OPTIONAL) Enter the keyword `md5` or `sha` to designate the authentication level. • `md5` — Message Digest Algorithm • `sha` — Secure Hash Algorithm
auth-password	(OPTIONAL) Enter a text string (up to 20 characters long) password that enables the agent to receive packets from the host. Minimum: 8 characters long.
priv des56	(OPTIONAL) Enter the keywords `priv des56` to initiate a privacy authentication level setting using the CBC-DES privacy authentication algorithm (des56).
priv password	(OPTIONAL) Enter a text string (up to 20 characters long) password that enables the host to encrypt the contents of the message it sends to the agent. Minimum: 8 characters long.
access *access-list-name*	(Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).
ipv6 *access-list-name*	(Optional) Enter the keyword `ipv6` followed by the IPv6 access list name (a string up to 16 characters long).
access-list-name ipv6 access-list-name	(Optional) Enter both an IPv4 and IPv6 access list name.

Defaults

As above.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

NOTE: For IPv6 ACLs, only IPv6 and UDP types are valid for SNMP. TCP and ICMP rules are not valid for SNMP. In IPv6 ACLs port rules are not valid for SNMP.

No default values exist for authentication or privacy algorithms and no default password exists. If you forget a password, you cannot recover it; the user must be reconfigured. You can specify either a plain-text password or an encrypted cypher-text password. In either case, the password is stored in the configuration in an encrypted form and displayed as encrypted in the `show running-config` command.

If you have an encrypted password, you can specify the encrypted string instead of the plain-text password. The following command is an Example of how to specify the command with an encrypted string.

NOTE: The number of configurable users is limited to 16.

Example

```
FTOS# snmp-server user privuser v3group v3 encrypted auth md5
9fc53d9d908118b2804fe80e3ba8763d priv des56
d0452401a8c3ce42804fe80e3ba8763d
```

Usage Information

The following command is an example of how to enter a plain-text password as the string `authpasswd` for user `authuser` of group `v3group`.

Example

```
FTOS#conf
FTOS(conf)# snmp-server user authuser v3group v3 auth md5
authpasswd
```

Usage Information

The following command configures a remote user named *n3user* with a v3 security model and a security level of `authNOPriv`.

Example

```
FTOS#conf
FTOS(conf)# snmp-server user n3user ngroup remote 172.31.1.3
udp-port 5009 3
auth md5 authpasswd
```

Related Commands

show snmp user – displays the information configured on each SNMP user name.

snmp-server view

Configure an SNMPv3 view.

S5000

Syntax

`snmp-server view *view-name oid-tree* {included | excluded}`

To remove an SNMPv3 view, use the `no snmp-server view view-name oid-tree {included | excluded}` command.

Parameters

view-name	Enter the name of the view (not to exceed 20 characters).
oid-tree	Enter the OID sub tree for the view (not to exceed 20 characters).
included	(OPTIONAL) Enter the keyword `included` to include the MIB family in the view.
excluded	(OPTIONAL) Enter the keyword `excluded` to exclude the MIB family in the view.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `oid-tree` variable is a full sub-tree starting from 1.3.6 and can not specify the name of a sub-tree or a MIB. The following Example configures a view named *rview* that allows access to all objects under 1.3.6.1.

Example

```
FTOS# conf
FTOS#(conf) snmp-server view rview 1.3.6.1 included
```

Related Commands

show running-config snmp – displays the SNMP running configuration.

snmp trap link-status

Enable the interface to send SNMP link traps, which indicate whether the interface is up or down.

S5000

Syntax

`snmp trap link-status`

To disable sending link trap messages, use the `no snmp trap link-status` command.

Defaults

Enabled.

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If the interface is expected to flap during normal usage, you could disable this command.

Syslog Commands

The following commands allow you to configure logging functions on all Dell Networking switches.

clear logging

Clear the messages in the logging buffer.

S5000

Syntax

`clear logging`

Defaults

none

Command Modes

EXEC Privilege

Command History	**Version 9.0(1.3)**	Introduced on the S5000.
Related Commands	show logging – displays logging settings and system messages in the internal buffer.	

default logging buffered

Return to the default setting for messages logged to the internal buffer.

S5000

Syntax	`default logging buffered`	
Defaults	**size = 40960; level = 7 or debugging**	
Command Modes	CONFIGURATION	
Command History	**Version 9.0(1.3)**	Introduced on the S5000.
Related Commands	logging buffered – sets the logging buffered parameters.	

default logging console

Return the default settings for messages logged to the console.

S5000

Syntax	`default logging console`	
Defaults	**level = 7 or debugging**	
Command Modes	CONFIGURATION	
Command History	**Version 9.0(1.3)**	Introduced on the S5000.
Related Commands	logging console – sets the logging console parameters.	

default logging monitor

Return to the default settings for messages logged to the terminal.

S5000

Syntax	`default logging monitor`
Defaults	**level = 7 or debugging**
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	logging monitor – sets the logging monitor parameters. terminal monitor – sends system messages to the terminal/monitor.

default logging trap

Return to the default settings for logging messages to the Syslog servers.

S5000

Syntax	`default logging trap`
Defaults	**level = 6 or informational**
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	logging trap – limit messages logged to the Syslog servers based on severity.

logging

Configure an IP address or host name of a Syslog server where logging messages are sent. Multiple logging servers of both IPv4 and/or IPv6 can be configured.

S5000

Syntax

`logging {ipv4-address | ipv6-address | hostname}`

To disable logging, use the `no logging` command.

Parameters

ipv4-address | ipv6-address	Enter an IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X) address.
hostname	Enter the name of a host already configured and recognized by the switch.

Defaults Disabled.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

logging on – enables the logging asynchronously to logging buffer, console, Syslog server, and terminal lines.

logging trap – enables logging to the Syslog server based on severity.

logging buffered

Enable logging and specify which messages are logged to an internal buffer. By default, all messages are logged to the internal buffer.

S5000

Syntax `logging buffered [level] [size]`

To return to the default values, use the `default logging buffered` command.

To disable logging stored to an internal buffer, use the `no logging buffered` command.

Parameters

level	(OPTIONAL) Indicate a value from 0 to 7 or enter one of the following equivalent words: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **7** or **debugging**.
size	(OPTIONAL) Indicate the size, in bytes, of the logging buffer. The number of messages buffered depends on the size of each message. The range is 40960 to 524288. The default is **40960 bytes**.

Defaults level = **7**; size = **40960 bytes**

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you decrease the buffer size, all messages stored in the buffer are lost. Increasing the buffer size does not affect messages stored in the buffer.

Related Commands

clear logging – clears the logging buffer.

default logging buffered – returns the logging buffered parameters to the default setting.

show logging – displays the logging setting and system messages in the internal buffer.

logging console

Specify which messages are logged to the console.

S5000

Syntax

`logging console [level]`

To return to the default values, use the `default logging console` command.

To disable logging to the console, use the `no logging console` command.

Parameters

level	(OPTIONAL) Indicate a value from 0 to 7 or enter one of the following parameters: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **7** or **debugging**.

Defaults

level = **7**; size = **debugging**

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

clear logging – clears the logging buffer.

default logging console – returns the logging console parameters to the default setting.

show logging – displays the logging setting and system messages in the internal buffer.

logging facility

Configure the Syslog facility used for error messages sent to Syslog servers.

S5000

Syntax

`logging facility [facility-type]`

To return to the default values, use the `no logging facility` command.

Parameters

facility-type	(OPTIONAL) Enter one of the following parameters: • `auth` (authorization system)

- `cron` (Cron/at facility)
- `deamon` (system deamons)
- `kern` (kernel)
- `local0` (local use)
- `local1` (local use)
- `local2` (local use)
- `local3` (local use)
- `local4` (local use)
- `local5` (local use)
- `local6` (local use)
- `local7` (local use)
- `lpr` (line printer system)
- `mail` (mail system)
- `news` (USENET news)
- `sys9` (system use)
- `sys10` (system use)
- `sys11` (system use)
- `sys12` (system use)
- `sys13` (system use)
- `sys14` (system use)
- `syslog` (Syslog process)
- `user` (user process)
- `uucp` (Unix to Unix copy process)

The default is **local7**.

Defaults local7

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

logging – enables logging to a Syslog server.

logging on – enables logging.

logging history

Specify which messages are logged to the history table of the switch and the SNMP network management station (if configured).

S5000

Syntax

`logging history level`

To return to the default values, use the `no logging history` command.

Parameters

level	Indicate a value from 0 to 7 or enter one of the following equivalent words: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **4** or **warnings**.

Defaults

warnings or 4

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you configure the `snmp-server trap-source` command, the system messages logged to the history table are also sent to the SNMP network management station.

Related Commands

show logging – displays information logged to the history buffer.

logging history size

Specify the number of messages stored in the FTOS logging history table.

S5000

Syntax

`logging history size size`

To return to the default values, use the `no logging history size` command.

Parameters

size	Indicate a value as the number of messages to be stored. The range is 0 to 500. The default is **1 message**.

Defaults

1 message

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	When the number of messages reach the limit you set with the `logging history size` command, older messages are deleted as newer ones are added to the table.
Related Commands	show logging – displays information logged to the history buffer.

logging monitor

Specify which messages are logged to Telnet applications.

S5000

Syntax

`logging monitor [level]`

To disable logging to terminal connections, use the `no logging monitor` command.

Parameters

level	Indicate a value from 0 to 7 or enter one of the following parameters: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **7** or **debugging**.

Defaults	**7** or **debugging**
Command Modes	CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands	default logging monitor – returns the logging monitor parameters to the default setting.

logging on

Specify that debug or error messages are asynchronously logged to multiple destinations, such as the logging buffer, Syslog server, or terminal lines.

S5000

Syntax

`logging on`

To disable logging to logging buffer, Syslog server and terminal lines, use the `no logging on` command.

Defaults	Enabled.
Command Modes	CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you use the `no logging on` command, messages are logged only to the console.

Related Commands

logging – enables logging to the Syslog server.

logging buffered – sets the logging buffered parameters.

logging console – sets the logging console parameters.

logging monitor – sets the logging parameters for the terminal connections.

logging source-interface

Specify that the IP address of an interface is the source IP address of Syslog packets sent to the Syslog server.

S5000

Syntax

`logging source-interface interface`

To disable this command and return to the default setting, use the `no logging source-interface` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information. • For Loopback interfaces, enter the keyword `loopback` followed by a number from zero (0) to 16383. • For the management interface, enter the keyword `ManagementEthernet` followed by the slot/port information. The slot range is 0 to 1 and the port range is 0. • For a Port Channel interface, enter the keywords `port-channel` followed by a number. The range is 1 to 128. • For VLAN interface, enter the keyword `vlan` followed by a number from 1 to 4094.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information	Syslog messages contain the IP address of the interface used to egress the router. By configuring the `logging source-interface` command, the Syslog packets contain the IP address of the interface configured.
Related Commands	logging – enables logging to the Syslog server.

logging synchronous

Synchronize unsolicited messages and FTOS output.

S5000

Syntax

`logging synchronous [level` *`level`* `| all] [limit` *`number-of-buffers`*`]`

To disable message synchronization, use the `no logging synchronous [level` *`level`* `| all] [limit` *`number-of-buffers`*`]` command.

Parameters

all	Enter the keyword `all` to ensure that all levels are printed asynchronously.
level *level*	Enter the keyword `level` followed by a number as the severity level. A high number indicates a low severity level and visa versa. The range is 0 to 7. The default is **2**.
all	Enter the keyword `all` to turn off all.
limit *number-of-buffers*	Enter the keyword `limit` followed by the number of buffers to be queued for the terminal after which new messages are dropped. The range is 20 to 300. The default is **20**.

Defaults

Disabled. If enabled without the `level` or `number-of-buffers` options specified, level = **2** and number-of-buffers = **20** are the defaults.

Command Modes

LINE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you enable `logging synchronous`, unsolicited messages appear between software prompts and outputs. Only the messages with a severity at or below the set level are sent to the console.

If the message queue limit is reached on a terminal line and messages are discarded, a system message appears on that terminal line. Messages may continue to appear on other terminal lines.

Related Commands

logging on – enables logging.

logging trap

Specify which messages are logged to the Syslog server based the message severity.

S5000

Syntax	`logging trap [level]` To return to the default values, use the `default logging trap` command. To disable logging, use the `no logging trap` command.
Parameters	***level*** — Indicate a value from 0 to 7 or enter one of the following parameters: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **6** or **informational**.
Defaults	**6** or **informational**
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** — Introduced on the S5000.
Usage Information	To block a type of message parameter, set the logging trap level to a lower number. For example, to block severity messages at level 6, set the level to 5.
Related Commands	logging – enables the logging to another device. logging on – enables logging.

show logging

Display the logging settings and system messages logged to the internal buffer of the switch.

S5000

Syntax

```
show logging [number | history [reverse][number] | reverse
[number] | summary]
```

Parameters

number	(OPTIONAL) Enter the number of message to be displayed on the output. The range is 1 to 65535.
history	(OPTIONAL) Enter the keyword `history` to view only information in the Syslog history table.
reverse	(OPTIONAL) Enter the keyword `reverse` to view the Syslog messages in FIFO (first in, first out) order.
summary	(OPTIONAL) Enter the keyword `summary` to view a table showing the number of messages per type and per slot.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (partial)

```
FTOS#show logging
Syslog logging: enabled
    Console logging: level debugging
    Monitor logging: level debugging
    Buffer logging: level debugging, 50 Messages Logged, Size
(40960 bytes)
    Trap logging: level informational
        Logging to 172.16.1.162
        Logging to 10.10.10.4
        Logging to 10.1.2.4
        Logging to 172.31.1.4
        Logging to 133.33.33.4
Apr 30 11:14:33: %STKUNIT1-M:CP %SYS-5-CONFIG_I: Configured
from vty0 ( 10.11.51.14 )by admin
Apr 30 10:13:08: %STKUNIT1-M:CP %SYS-5-CONFIG_I: Configured
from vty0 ( 10.11.51.14 )by admin
Apr 30 10:06:41: %STKUNIT1-M:CP %SEC-3-
AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication
success on vty0 ( 10.11.51.14 )
Apr 30 10:06:36: %STKUNIT1-M:CP %SEC-5-LOGIN_SUCCESS: Login
successful for user admin on vty0 (10.11.51.14)
Apr 26 12:02:48: %S5000:1 %IFAGT-5-STACK_PORT_LINK_DOWN:
Changed stack port state to down: 1/56
Apr 26 11:52:45: %S5000:1 %IFAGT-5-STACK_PORT_LINK_UP: Changed
stack port state to up: 1/56
Apr 26 11:51:13: %S5000:1 %IFAGT-5-STACK_PORT_LINK_DOWN:
Changed stack port state to down: 1/56
Apr 26 11:51:01: %S5000:1 %IFAGT-5-STACK_PORT_LINK_DOWN:
Changed stack port state to down: 1/48
Apr 26 11:48:57: %S5000:1 %IFAGT-5-STACK_PORT_LINK_UP: Changed
stack port state to up: 1/56
Apr 26 11:48:47: %S5000:1 %IFAGT-5-STACK_PORT_LINK_UP: Changed
stack port state to up: 1/48
Apr 26 11:43:52: %S5000:1 %IFAGT-5-STACK_PORT_LINK_DOWN:
Changed stack port state to down: 1/48
Apr 26 11:43:43: %S5000:1 %IFAGT-5-STACK_PORT_LINK_DOWN:
Changed stack port state to down: 1/56
Apr 26 11:33:08: %S5000:1 %IFAGT-5-STACK_PORT_LINK_UP: Changed
stack port state to up: 1/48
Apr 26 11:33:08: %S5000:1 %IFAGT-5-STACK_PORT_LINK_UP: Changed
stack port state to up: 1/56
Apr 25 11:07:15: %S5000:1 %IFAGT-5-REMOVED_OPTICS_PLUS: Optics
SFP+ removed in slot 1 port 2
Apr 25 11:07:14: %S5000:1 %IFAGT-5-REMOVED_OPTICS_PLUS: Optics
SFP+ removed in slot 1 port 3
!------------------ output truncated ------------------!
```

Example (history)

```
FTOS#show logging history
Syslog History Table: 1 maximum table entries,
saving level warnings or higher
SNMP notifications not Enabled
Apr 30 10:06:41: %STKUNIT1-M:CP %SEC-3-
```

```
AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication
success on vty0 ( 10.11.51.14 )
```

show logging driverlog stack-unit

Display the driver log for the specified stack member.

S5000

Syntax `show logging driverlog stack-unit` *`unit-number`*

Parameters

stack-unit *unit-number*	Enter the keywords `stack-unit` followed by the unit number. The range is 0 to 11.

defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This command displays internal software driver information, which may be useful during troubleshooting switch initialization errors, such as a downed Port-Pipe.

terminal monitor

Configure the FTOS to display messages on the monitor/terminal.

S5000

Syntax `terminal monitor`

To return to default settings, use the `terminal no monitor` command.

defaults Disabled.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands	logging monitor – sets the logging parameters on the monitor/terminal.

52

Spanning Tree Protocol (STP)

The commands in this chapter configure and monitor the IEEE 802.1d spanning tree protocol (STP) and are supported on the S5000 switch.

bridge-priority

Set the bridge priority of the switch in an IEEE 802.1D spanning tree.

S5000

Syntax

```
bridge-priority {priority-value | primary | secondary}
```

To return to the default value, use the `no bridge-priority` command.

Parameters

priority-value	Enter a number as the bridge priority value. The range is 0 to 65535. The default is **32768**.
primary	Enter the keyword `primary` to designate the bridge as the root bridge.
secondary	Enter the keyword `secondary` to designate the bridge as a secondary root bridge.

Defaults priority-value = **32768**

Command Modes SPANNING TREE (The prompt is “config-stp”.)

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug spanning-tree

Enable debugging of the spanning tree protocol and view information on the protocol.

S5000

Syntax

```
debug spanning-tree {stp-id [all | bpdu | config | events |
exceptions | general | root] | protocol}
```

To disable debugging, use the `no debug spanning-tree` command.

Parameters

stp-id	Enter zero (0). The switch supports one spanning tree group with a group ID of 0.
protocol	Enter the keyword for the type of STP to debug, either `mstp`, `pvst`, or `rstp`.
all	(OPTIONAL) Enter the keyword `all` to debug all spanning tree operations.
bpdu	(OPTIONAL) Enter the keyword `bpdu` to debug bridge protocol data units.
config	(OPTIONAL) Enter the keyword `config` to debug configuration information.
events	(OPTIONAL) Enter the keyword `events` to debug STP events.
general	(OPTIONAL) Enter the keyword `general` to debug general STP operations.
root	(OPTIONAL) Enter the keyword `root` to debug STP root transactions.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information When you enable `debug spanning-tree bpdu` for multiple interfaces, the software only sends information on BPDUs for the last interface specified.

Related Commands protocol spanning-tree – enters SPANNING TREE mode on the switch.

description

Enter a description of the spanning tree.

S5000

Syntax `description {`*`description`*`}`

To remove the description from the spanning tree, use the `no description {`*`description`*`}` command.

Parameters

description	Enter a description to identify the Spanning Tree (80 characters maximum).

Defaults none

Command Modes SPANNING TREE (The prompt is “config-stp”.)

Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	protocol spanning-tree – enters SPANNING TREE mode on the switch.

disable

Disable the spanning tree protocol globally on the switch.

S5000

Syntax	`disable` To enable Spanning Tree Protocol, use the `no disable` command.
Defaults	Enabled (that is, the spanning tree protocol is disabled.)
Command Modes	SPANNING TREE
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	protocol spanning-tree – enters SPANNING TREE mode on the switch.

forward-delay

The amount of time the interface waits in the Listening state and the Learning state before transitioning to the Forwarding state.

S5000

Syntax	`forward-delay` *`seconds`* To return to the default setting, use the `no forward-delay` command.
Parameters	***seconds*** Enter the number of seconds the FTOS waits before transitioning STP to the Forwarding state. The range is 4 to 30. The default is **15 seconds**.
Defaults	**15 seconds**
Command Modes	SPANNING TREE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Related Commands	max-age – changes the wait time before STP refreshes protocol configuration information. hello-time – changes the time interval between BPDUs.

hello-time

Set the time interval between generation of the spanning tree bridge protocol data units (BPDUs).

S5000

Syntax `hello-time seconds`

To return to the default value, use the `no hello-time` command.

Parameters

seconds	Enter a number as the time interval between transmission of BPDUs. The range is 1 to 10. The default is **2 seconds**.

Defaults 2 seconds

Command Modes SPANNING TREE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands	forward-delay – changes the wait time before STP transitions to the Forwarding state. max-age – changes the wait time before STP refreshes protocol configuration information.

max-age

Set the time interval for the spanning tree bridge to maintain configuration information before refreshing that information.

S5000

Syntax `max-age seconds`

To return to the default values, use the `no max-age` command.

Parameters

seconds	Enter a number of seconds the FTOS waits before refreshing configuration information. The range is 6 to 40. The default is **20 seconds**.

Defaults 20 seconds

Command Modes SPANNING TREE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

forward-delay – changes the wait time before STP transitions to the Forwarding state.

hello-time – changes the time interval between BPDUs.

protocol spanning-tree

Enter SPANNING TREE mode to enable and configure the spanning tree group.

S5000

Syntax

`protocol spanning-tree stp-id`

To disable the Spanning Tree group, use the `no protocol spanning-tree stp-id` command.

Parameters

stp-id	Enter zero (0). FTOS supports one spanning tree group, group 0.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

STP is not enabled when you enter SPANNING TREE mode. To enable STP globally on the switch, use the `no disable` command from SPANNING TREE mode.

Example

```
FTOS(conf)#protocol spanning-tree 0
FTOS(config-stp)#
```

Related Commands

disable – disables spanning tree group 0. To enable spanning tree group 0, use the `no disable` command.

show config

Display the current configuration for the mode. Only non-default values are displayed.

S5000

Syntax

`show config`

Command Modes

SPANNING TREE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(config-stp)#show config
protocol spanning-tree 0
  no disable
FTOS(config-stp)#
```

show spanning-tree 0

Display the spanning tree group configuration and status of interfaces in the spanning tree group.

S5000

Syntax `show spanning-tree 0 [active | brief | guard | interface type slot/port | root | summary]`

Parameters

0	Enter `0` (zero) to display information about that specific spanning tree group.
active	(OPTIONAL) Enter the keyword `active` to display only active interfaces in spanning tree group 0.
brief	(OPTIONAL) Enter the keyword `brief` to display a synopsis of the spanning tree group configuration information.
guard	(OPTIONAL) Enter the keyword `guard` to display the type of guard enabled on an STP interface and the current port state.
interface *type slot/port*	(OPTIONAL) Enter the keyword `interface` and the type slot/port of the interface you want displayed. Type slot/port options are the following: • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
root	(OPTIONAL) Enter the keyword `root` to display configuration information on the spanning tree group root.
summary	(OPTIONAL) Enter the keyword `summary` to only the number of ports in the spanning tree group and their state.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must enable spanning tree group 0 prior to using this command.

The following describes the `show spanning-tree 0` command shown in the Example below.

Field	Description
Bridge Identifier...	Lists the bridge priority and the MAC address for this STP bridge.
Configured hello...	Displays the settings for hello time, max age, and forward delay.
We are...	States whether this bridge is the root bridge for the STG.
Current root...	Lists the bridge priority and MAC address for the root bridge.
Topology flag...	States whether the topology flag and the detected flag were set.
Number of...	Displays the number of topology changes, the time of the last topology change, and on what interface the topology change occurred.
Timers	Lists the values for the following bridge timers: hold time, topology change, hello time, max age, and forward delay.
Times	List the number of seconds since the last: • hello time • topology change • notification • aging
Port 1...	Displays the Interface type slot/port information and the status of the interface (Disabled or Enabled).
Port path...	Displays the path cost, priority, and identifier for the interface.
Designated root...	Displays the priority and MAC address of the root bridge of the STG that the interface belongs.
Designated port...	Displays the designated port ID.

Example

```
FTOS#show spann 0

Executing IEEE compatible Spanning Tree Protocol
 Bridge Identifier has priority 32768, Address 0001.e800.0a56
 Configured hello time 2, max age 20, forward delay 15
 We are the root of the spanning tree
 Current root has priority 32768 address 0001.e800.0a56
 Topology change flag set, detected flag set
 Number of topology changes 1 last change occurred 0:00:05 ago
   from TenGigabitEthernet 1/3
 Timers:hold 1, topology change 35
        hello 2, max age 20, forward_delay 15
 Times:hello 1, topology change 1, notification 0, aging 2

Port 26 (TenGigabitEthernet 1/1) is Forwarding
```

```
 Port path cost 4, Port priority 8, Port Identifier 8.26
 Designated root has priority 32768, address 0001.e800.0a56
 Designated bridge has priority 32768, address 0001.e800.0a56
 Designated port id is 8.26, designated path cost 0
 Timers: message age 0, forward_delay 0, hold 0
 Number of transitions to forwarding state 1
 BPDU: sent:18, received 0
 The port is not in the portfast mode

Port 27 (TenGigabitEthernet 1/2) is Forwarding
 Port path cost 4, Port priority 8, Port Identifier 8.27
 Designated root has priority 32768, address 0001.e800.0a56
 Designated bridge has priority 32768, address 0001.e800.0a56
 Designated port id is 8.27, designated path cost 0
 Timers: message age 0, forward_delay 0, hold 0
 Number of transitions to forwarding state 1
 BPDU: sent:18, received 0
 The port is not in the portfast mode

Port 28 (TenGigabitEthernet 1/3) is Forwarding
 Port path cost 4, Port priority 8, Port Identifier 8.28
 Designated root has priority 32768, address 0001.e800.0a56
 Designated bridge has priority 32768, address 0001.e800.0a56
 Designated port id is 8.28, designated path cost 0
 Timers: message age 0, forward_delay 0, hold 0
 Number of transitions to forwarding state 1
 BPDU: sent:31, received 0
 The port is not in the portfast mode

FTOS#
```

Example (Brief)

```
FTOS#show span 0 brief
  Executing IEEE compatible Spanning Tree Protocol
    Root ID Priority 32768
      Address 0001.e800.0a56
    Root Bridge hello time 2, max age 20, forward delay 15
    Bridge ID Priority 32768,
      Address 0001.e800.0a56
    Configured hello time 2, max age 20, forward delay 15
Interface                        Designated
Name   PortID Prio Cost Sts Cost Bridge ID            PortID
-------------- ------ ---- ---- --- ----- ------------------
Te 1/1 8.26   8    4     FWD 0    32768 0001.e800.0a56 8.26
Te 1/2 8.27   8    4     FWD 0    32768 0001.e800.0a56 8.27
Te 1/3 8.28   8    4     FWD 0    32768 0001.e800.0a56 8.28
FTOS#
```

Usage Information

The following describes the `show spanning-tree 0 guard` command shown in the Example below.

Field	Description
Interface Name	STP interface.
Instance	STP 0 instance.
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard).

Example (Guard)

```
FTOS#show spanning-tree 0 guard
Interface
Name   Instance Sts          Guard type
--------- -------- --------- ----------
Te 0/1 0        INCON(Root)  Rootguard
Te 0/2 0        LIS          Loopguard
Te 0/3 0        EDS (Shut)   Bpduguard
```

spanning-tree 0

Assigns a Layer 2 interface to STP instance 0 and configures a port cost or port priority, or enables loop guard, root guard, or the Portfast feature on the interface.

S5000

Syntax

```
spanning-tree stp-id {cost cost | {loopguard | rootguard} |
portfast [bpduguard [shutdown-on-violation]] | priority
priority}
```

To disable Spanning Tree group on an interface, use the `no spanning-tree stp-id {cost cost | {loopguard | rootguard} | portfast [bpduguard [shutdown-on-violation]] | priority priority}` command.

Parameters

stp-id	Enter the STP instance ID. The range is 0.
cost *cost*	Enter the keyword `cost` followed by a number as the cost. The range is 1 to 65535. The defaults are: - Gigabit Ethernet interface = **4**. - 10-Gigabit Ethernet interface = **2**. - 40-Gigabit Ethernet interface = **2**. - Port Channel interface with Gigabit Ethernet = **3**. - Port Channel interface with 10-Gigabit Ethernet = **1**. - Port Channel interface with 40-Gigabit Ethernet = **1**.
loopguard	Enter the keyword `loopguard` to enable STP loop guard on a port or port-channel interface.
rootguard	Enter the keyword `rootguard` to enable STP root guard on a port or port-channel interface.
portfast [bpduguard [shutdown-on-viol ation]]	Enter the keyword `portfast` to enable Portfast to move the interface into Forwarding mode immediately after the root fails. Enter the optional keyword `bpduguard` to disable the port when it receives a BPDU. Enter the optional keyword `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.

priority *priority*	Enter keyword `priority` followed by a number as the priority. The range is zero (0) to 15. The default is **8**.

Defaults cost = depends on the interface type; priority = **8**

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

If you enable `portfast bpduguard` on an interface and the interface receives a BPDU, the software disables the interface and sends a message stating that fact. The port is in ERR_DISABLE mode, yet appears in the `show interface` commands as enabled. If you do not enable `shutdown-on-violation`, BPDUs are still sent to the stack-unit CPU.

STP loop guard and root guard are supported on a port or port-channel enabled in any Spanning Tree mode: Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and Per-VLAN Spanning Tree Plus (PVST+).

Root guard is supported on any STP-enabled port or port-channel except when used as a stacking port. When enabled on a port, root guard applies to all VLANs configured on the port.

STP root guard and loop guard cannot be enabled at the same time on a port. For example, if you configure loop guard on a port on which root guard is already configured, the following error message is displayed: `% Error: RootGuard is configured. Cannot configure LoopGuard`.

Do not enable Portfast BPDU guard and loop guard at the same time on a port. Enabling both features may result in a port that remains in a blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an Err-Disabled Blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a Loop-Inconsistent Blocking state and no traffic is forwarded on the port.

To display the type of STP guard (Portfast BPDU, root, or loop guard) enabled on a port, enter the `show spanning-tree 0` command.

53

Stacking Commands

All commands in this chapter are specific to the Dell Networking operating software (FTOS) on the S5000 switch.

The commands are always available and operational. You can use the commands to pre-configure a switch so that the configuration settings are invoked when the switch is attached to other S5000 units.

For information about using the S5000 stacking feature, refer to the Stacking chapter in the *FTOS Configuration Guide* for the S5000.

⚠ **CAUTION: You cannot enable S5000 stacking simultaneously with virtual link trunking (VLT). If you enable both at the same time, unexpected behavior occurs.**

redundancy disable-auto-reboot stack-unit

Prevent the S5000 stack management unit, stack member unit, and standby unit from rebooting if they fail.

S5000

Syntax

```
redundancy disable-auto-reboot stack-unit [members | 0-11]
```

To re-enable the automatic reboot of a failed stack unit, use the `no redundancy disable-auto-reboot stack-unit` command.

Defaults Disabled (a failed switch automatically reboots).

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The range is 0 to 11. Entering this command disables the automatic reboot and keeps a failed stack unit in the Failed state. A failed switch does not reboot until you manually reload it. The disabling of the automatic reboot is displayed in the running-config.

Related Commands show redundancy – displays the current redundancy status.

redundancy force-failover stack-unit

Force the standby unit in the stack to become the management unit.

S5000

Syntax `redundancy force-failover stack-unit`

Defaults Not enabled.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

reset stack-unit

Reset any designated stack member except the management unit (master unit).

S5000

Syntax `reset stack-unit` *`unit-number`* `hard`

Parameters

unit-number	Enter the stack-unit number. The range is 0 to 11.
hard	Reset the stack unit if the unit is in a problem state.

Defaults none

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Resetting the management unit is not allowed, and an error message displays if you try to do so. Resetting is a soft reboot, including flushing the forwarding tables.

You can run this command directly on the stack standby unit (standby master) to reset the standby. You cannot reset any other unit from the standby unit.

Example

```
FTOS#reset stack-unit 4
Apr 8 10:22:43: %STKUNIT3-M:CP %CHMGR-5-STACKUNIT_RESET: Stack
unit 4 being reset
Apr 8 10:22:43: %STKUNIT3-M:CP %IFMGR-5-OSTATE_DN: Changed
interface state to down: Te 4/0
Apr 8 10:22:43: %STKUNIT3-M:CP %IFMGR-5-OSTATE_DN: Changed
interface state to down: Te 4/20
Apr 8 10:22:43: %STKUNIT3-M:CP %IFMGR-5-OSTATE_DN: Changed
interface state to down: Te 4/21
Apr 8 10:22:44: %STKUNIT3-M:CP %IFMGR-5-OSTATE_DN: Changed
interface state to down: Te 4/22
Apr 8 10:22:44: %STKUNIT3-M:CP %IFMGR-5-OSTATE_DN: Changed
interface state to down: Te 4/23
FTOS#Apr 8 10:22:44: %STKUNIT3-M:CP %IFMGR-5-OSTATE_DN:
```

```
Changed interface state to down: Po 102
Apr 8 10:22:44: %STKUNIT3-M:CP %IFMGR-1-DEL_PORT: Removed
port: Te 4/0-3,16-47, Fo 4/48,52,60,
Apr 8 10:22:44: %STKUNIT3-M:CP %CHMGR-2-STACKUNIT_DOWN: Stack
unit 4 down - reset
Apr 8 10:22:44: %STKUNIT2-S:CP %IFMGR-1-DEL_PORT: Removed
port: Te 4/0-3,16-47, Fo 4/48,52,60,
Apr 8 10:22:50: %S5000:3 %IFAGT-5-STACK_PORT_LINK_DOWN:
Changed stack port state to down: 3/12
```

Related Commands

- reload – reboots FTOS.
- upgrade system stack-unit – synchronizes the FTOS image running on an S5000 stack unit from the master switch.

show redundancy

Display the current redundancy configuration (status of automatic reboot configuration on stack management unit).

S5000

Syntax `show redundancy`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show redundancy

--  Stack-unit Status  --
------------------------------------------------
Mgmt ID:                          0
Stack-unit ID:                    4
Stack-unit Redundancy Role:       Primary
Stack-unit State:                 Active
 Stack-unit SW Version:            9.0(1.3)
Link to Peer:                     Up

--  PEER Stack-unit Status  --
------------------------------------------------
Stack-unit State:                 Standby
Peer stack-unit ID:               3
Stack-unit SW Version:            9.0(1.0)

--  Stack-unit Redundancy Configuration  --
------------------------------------------------
Primary Stack-unit:               mgmt-id    0
Auto Data Sync:                   Full
Failover Type:                    Hot Failover
Auto reboot Stack-unit:           Disabled
Auto failover limit:              3 times in 60 minutes
```

```
--  Stack-unit Failover Record  --
------------------------------------------------
Failover Count:                   0
Last failover timestamp:          None
Last failover Reason:             None
Last failover type:               None

--  Last Data Block Sync Record:  --
------------------------------------------------
Stack Unit Config:          succeeded  Apr 17 2013 09:07:10
   Start-up Config:          succeeded  Apr 17 2013 09:07:10
 Runtime Event Log:          succeeded  Apr 17 2013 09:07:10
    Running Config:          succeeded  Apr 17 2013 09:07:10
           ACL Mgr:          succeeded  Apr 17 2013 09:07:10
              LACP:          no block sync done
               STP:          no block sync done
              SPAN:          no block sync done
FTOS#
```

Related Commands

redundancy disable-auto-reboot – prevents the system from auto-rebooting if it fails.

show system stack-ports

Display information about the stacking ports on all switches in the S5000 stack.

S5000

Syntax

`show system stack-ports [status | topology]`

Parameters

status	(OPTIONAL) Enter the keyword `status` to display the command output without the Connection field.
topology	(OPTIONAL) Enter the keyword `topology` to limit the table to just the Interface and Connection fields.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output from the `show system stack-ports` command shown in the Example below.

Field	Description
Topology	Lists the topology of stack ports connected: Ring, Daisy chain, or Standalone.

Interface	The unit/port ID of the connected stack port on this unit.
Connection	The stack port to which this unit’s stack port is connected.
Link Speed	Link speed of the stack port (10 or 40) in Gb/s.
Admin Status	The only currently listed status is “up”.
Link Status	Status of the link between stack ports: up or down.

Example

```
FTOS# show system stack-ports
Topology: Ring
Interface Connection Link Speed Admin  Link
                       (Gb/s)   Status Status
--------------------------------------------------
0/4         1/4          10      up     up
0/5         1/5          10      up     up
0/6         1/6          10      up     up
0/7         1/7          10      up     up
0/8         4/12         10      up     up
0/9         4/13         10      up     up
0/10        4/14         10      up     up
0/11        4/15         10      up     up
1/4         0/4          10      up     up
1/5         0/5          10      up     up
1/6         0/6          10      up     up
1/7         0/7          10      up     up
FTOS#
```

Example (Status)

```
FTOS# show system stack-ports status
Topology: Ring
Interface Link Speed Admin  Link
           (Gb/s)    Status Status
----------------------------------------
0/4          10      up     up
0/5          10      up     up
0/6          10      up     up
0/7          10      up     up
0/8          10      up     up
0/9          10      up     up
0/10         10      up     up
0/11         10      up     up
1/4          10      up     up
1/5          10      up     up
1/6          10      up     up
1/7          10      up     up
FTOS#
```

Example (Topology)

```
FTOS# show system stack-ports topology

Topology: Ring

Interface Connection   Trunk
                       Group
----------------------------
  0/4        1/4
  0/5        1/5
  0/6        1/6
  0/7        1/7
  0/8        4/12
  0/9        4/13
  0/10       4/14
  0/11        4/15
  1/4         0/4
  1/5         0/5
  1/6         0/6
  1/7         0/7
  1/8         2/4
  1/9         2/5
  1/10        2/6
  1/11        2/7
FTOS#
```

Related Commands

- reset stack-unit – resets the designated S5000 stack member.
- show hardware stack-unit – displays the data plane or management plane input and output statistics of the designated component of the designated stack member.
- show system – displays the current status of all stack members or a specific member.
- upgrade (management unit) – upgrades the bootflash image or system image of the S5000 management unit.

show system stack-unit stack-group

Display the stacking group port information for the specified stack-unit.

S5000

Syntax

`show system stack-unit *unit-number* stack-group configured`

Parameters

stack-unit *unit-number* stack-group configured	Enter the `stack-unit` keyword followed by the unit number. The range is 0 to 11. Then enter `stack-group configured`.

Defaults

none

Command Modes

GLOBAL

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show system stack-unit 4 stack-group configured
Configured stack groups in stack-unit 4
------------------------------------------
12
13
```

stack-unit priority

Configure the ability of an S5000 switch to become the management unit of a stack.

S5000

Syntax `stack-unit unit-number priority priority-level`

Parameters

unit-number	Enter the stack-unit number. The range is 0 to 11.
priority *priority-level*	Specify the management priority assigned to the switch, where 1 is the lowest priority and 14 is the highest priority. The switch with the highest priority value is selected as the management unit if the active management unit fails or on the next reload.

Defaults 0

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

- reload – reboots FTOS.
- show system – displays the status of all stack members or a specific member.

stack-unit provision

Pre-configure a logical stack-unit number for an S5000 switch to join the stack. This is an optional command that is executed on the management unit.

S5000

Syntax `stack-unit unit-number provision S5000`

Parameters

unit-number	Enter the stack-unit number. The range is 0 to 11.
S5000	Enter the model identifier of the switch to be added as a stack member. This identifier is also referred to as the *provision type*.

Defaults None

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

- reload – reboots FTOS.

- show system – displays the status of all stack members or a specific member.

stack-unit renumber

Change the stack-unit number of any stack unit or a stand-alone S5000.

S5000

Syntax `stack-unit unit-number renumber unit-number`

Parameters

unit-number **renumber**	Enter the stack-unit number followed by the keyword `renumber`. The range is 0 to 11. The first instance of this value is the currently configured unit number of an S5000 switch. The second instance of this value is the new unit number to be assigned to the switch.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can renumber any switch, including the management unit or a stand-alone unit.

You cannot renumber a unit to a number of an active member in the stack.

When executing this command on the master, the stack reloads. When the members are renumbered, only that specific unit is reset and comes up with the new unit number.

Example

```
FTOS#stack-unit 5 renumber 6

Renumbering will reset the unit.
Warning: Interface configuration for current unit will be lost!
Proceed to renumber [confirm yes/no]:
```

Related Commands

- reload – reboots FTOS.
- reset stack-unit – resets the designated S5000 stack member.
- show system – displays the current status of all stack members or a specific member.

stack-unit stack-group

Configure the stack unit and stack group by specifying an ID when adding units to a stack to ensure the unit is assigned to the correct group.

S5000

Syntax

`stack-unit unit-number stack-group stack-group-number`

To remove the current stack group configuration, use the `no stack-unit unit-number stack-group stack-number` command.

Parameters

unit-number	Enter the stack-unit number. The range is 0 to 11.
stack-group-number	Enter the stack-group number. The range is 0 to 15.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following message displays to confirm the command.

WARNING: Setting ports Fo 0/60 as stack group will make their interface configs obsolete after a reload.[confirm yes/no]: If "y" is entered, all non-default configurations on this port (FortyGigE 0/60) will be removed when the unit reboots.

upgrade boot (stack unit)

Upgrade the boot image (bootflash or bootselector) on one or all stack units in an S5000 stack from the master switch.

S5000

Syntax

```
upgrade boot {bootflash-image| bootselector-image} stack-unit
{stack-unit—id | all} {booted: | flash://file-path | ftp://
file-path | tftp://file-path | usbflash://file-path}
```

Parameters

boot	Enter the keyword `boot` to change the boot image.
bootflash-image	Upgrade the boot image in the bootflash partition.
bootselector-image	Upgrade the boot image in the bootselector partition. You are prompted to enter the password.
stack-unit {*stack-unit-id* | all}	Enter the keyword `stack-unit:` followed by the stack unit ID of a member unit or `all` to upgrade the boot image on all stack member units. Valid stack-unit ID numbers are 0 to 11.

booted:	Upgrade the stack using the image with which the master switch booted up.
flash:	After the keyword `flash:`, enter the location of the source file in the internal flash in the format: `//`*`file-pathname`* or press **Enter** to launch a prompt sequence.
ftp:	After the keyword `ftp:`, enter the location of the source file in the format: `//`*`userid`*`:`*`password`*`@`*`host-ip-address`*`/`*`file-pathname`* or press **Enter** to launch a prompt sequence.
tftp:	After the keyword `tftp:`, enter the location of the source file in the format: `//`*`host-ipaddress`*`/`*`file—pathname`* or press **Enter** to launch a prompt sequence.
usbflash:	After the keyword `usbflash:`, enter the location of the source file in the format: `//`*`file-pathname`* or press **Enter** to launch a prompt sequence.
file-path	Enter the path and filename to be used to upgrade the boot image.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information You must reload the stack after entering the `upgrade boot stack-unit` command to boot up stack units with the new boot code.

Example

```
FTOS#upgrade boot bootselector-image stack-unit all booted

Password:

Current BootSelector information in the system:
===============================================================

Card       BootSelector    Current Version   New Version
---------------------------------------------------------------
Unit0      Boot Selector      1.3.0.0m        1.3.0.0m
Unit7      Boot Selector      1.3.0.0m        1.3.0.0m
Unit8      Boot Selector      1.3.0.0m        1.3.0.0m
Unit9      Boot Selector      1.3.0.0m        1.3.0.0m

***************************************************************
* Warning - Upgrading boot selectors is inherently risky and  *
* should only be attempted when necessary.  A failure at this *
* upgrade may cause a board RMA.  Proceed with caution !      *
***************************************************************

Proceed Boot Selector image for all units [yes/no]: yes


Programming
!.!.!.!.!!.!.!.!.!!.!.!.!.!.!.!!.!.!.!.!!.!.!.!.!.!!.!.!.!.!.!!
.!.
Bootselector image upgrade for all completed successfully.
FTOS#
```

```
FTOS#upgrade  boot bootflash-image  stack-unit all booted

Current BootFlash information in the system:
==============================================================

Card       BootFlash     Current Version   New Version
--------------------------------------------------------------
Unit0      Boot Flash B      1.3.1.1o        1.3.1.1p
Unit7      Boot Flash B      1.3.1.1o        1.3.1.1p
Unit8      Boot Flash A      1.3.1.1o        1.3.1.1p
Unit9      Boot Flash A      1.3.1.1o        1.3.1.1p

***************************************************************
*  Warning - Upgrading boot flash is inherently risky and     *
*  should only be attempted when necessary. A failure at this *
*  upgrade may cause a board RMA.  Proceed with caution !     *
***************************************************************

Proceed Boot Flash image for all units [yes/no]: yes
Programming
!!.!.!.!.!.!.!.!!.!.!.!.!.!!.!.!.!.!!.!.!.!.!.!!.!.!.!.!.!!.!.!
.!.!.!!.!.!.!.!.!!.!.!.!.!!.!.01:01:29: %STKUNIT7-M:CP
%SYSADM-5-CPU_THRESHOLD: Overall cpu usage of management-unit
is above threshold. Cpu1minUsage (89%)
01:01:29: %STKUNIT7-M:CP %SYSADM-5-TASK_CPU_THRESHOLD: 1min
cpu utilization of management-unit has exceeded the threshold.
Top three processes are sysdlp (79.79%), system (7.60%), sysd
(1.01%)
!.!.!.!!.01:01:34: %STKUNIT7-M:CP %SYSADM-5-CPU_THRESHOLD:
Overall cpu usage of stack-unit 10 is above threshold.
Cpu1minUsage (90%)
01:01:34: %STKUNIT7-M:CP %SYSADM-5-TASK_CPU_THRESHOLD: 1min
cpu utilization of stack-unit 10 has exceeded the threshold.
Top three processes are dla (88.75%), KP (2.50%), frrpaRecv
(0.00%)
!.!.!.!.!01:01:40: %STKUNIT7-M:CP %SYSADM-5-CPU_THRESHOLD:
Overall cpu usage of stack-unit 9 is above threshold.
Cpu1minUsage (96%)
01:01:40: %STKUNIT7-M:CP %SYSADM-5-TASK_CPU_THRESHOLD: 1min
cpu utilization of stack-unit 9 has exceeded the threshold.
Top three processes are dla (94.83%), KP (2.17%), frrpaRecv
(0.00%)
!.01:01:40: %STKUNIT7-M:CP %SYSADM-5-CPU_THRESHOLD: Overall
cpu usage of stack-unit 11 is above threshold. Cpu1minUsage
(96%)
01:01:40: %STKUNIT7-M:CP %SYSADM-5-TASK_CPU_THRESHOLD: 1min
cpu utilization of stack-unit 11 has exceeded the threshold.
Top three processes are dla (94.58%), KP (2.25%), frrpaRecv
(0.00%)
!.!.!.!.!01:01:45: %STKUNIT7-M:CP %SYSADM-5-CPU_THRESHOLD:
Overall cpu usage of stack-unit 0 is above threshold.
Cpu1minUsage (91%)
01:01:46: %STKUNIT7-M:CP %SYSADM-5-TASK_CPU_THRESHOLD: 1min
cpu utilization of stack-unit 0 has exceeded the threshold.
Top three processes are dla (89.75%), KP (2.67%), frrpaRecv
(0.00%)
!.!.!.!.!!.!.!.!.!!.!.!.!.!.!!.!.!.!.!!.!.!.!.!.!.!!.!.!.!.!.!!
.!.!.!.!.!!.!.!.!.!.!.!.!!.!.!.!.!!.!.!.!.!!.!.!.!.!.!.!!.!.!.!.!
.!!.!.!.!.!.!.!!.!.!.!.!.!!.!.!.!.!!.!.!.!.!.!
Bootflash image upgrade for all completed successfully.
```

upgrade system (stack unit)

Upgrade the FTOS image on one or all stack units in an S5000 stack from the master switch.

S5000

Syntax

```
upgrade system {flash://file-path | ftp://file-path | scp://
file-path | tftp://file-path | usbflash://file-path} | stack-
unit {stack-unit—id | all}{A: | B:}}
```

Parameters

boot	Enter the keyword `system` to change the FTOS image.
flash:	After the keyword `flash:`, enter the location of the source file in the internal flash in the format: `//`*`file-pathname`* or press **Enter** to launch a prompt sequence.
ftp:	After the keyword `ftp:`, enter the location of the source file in the format: `//`*`userid`*`:`*`password`*`@`*`host-ipaddress`*`/`*`file—pathname`* or press **Enter** to launch a prompt sequence.
scp:	After the keyword `scp:`, enter the location of the source file in the format: `//`*`userid`*`:`*`password`*`@`*`host-ip-address`*`/`*`file-pathname`* or press **Enter** to launch a prompt sequence.
tftp:	After the keyword `tftp:`, enter the location of the source file in the format: `//`*`host-ipaddress`*`/`*`file-pathname`* or press **Enter** to launch a prompt sequence.
usbflash:	After the keyword `usbflash:`, enter the location of the source file in the external flash in the format: `//`*`file-path`* or press **Enter** to launch a prompt sequence.
file-path	Enter the path and filename to be used to upgrade the FTOS image.
stack-unit {*stack-unit-id* | all}	Enter the keyword `stack-unit:` followed by the stack unit ID of a member unit or `all` to upgrade the boot image on all stack member units. Valid stack-unit ID numbers are 0 to 11.
A:* | *B:	Enter the FTOS partition to be upgraded with the new image.

Defaults None

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must reload FTOS after executing this command. Use the `upgrade system stack-unit` command to copy FTOS from the management unit to one or more stack members.

Example

```
FTOS#upgrade system ?
flash: Copy from flash file system (flash://filepath)
ftp: Copy from remote file system, IPv4 or IPv6, (ftp://
userid:password@hostip/filepath)
scp: Copy from remote file system, IPv4 or IPv6, (scp://
userid:password@hostip/filepath)
stack-unit: Sync image to the stack-unit
```

```
tftp: Copy from remote file system, IPv4 or IPv6, (tftp://
hostip/filepath)


FTOS#upgrade system ftp://username:password@10.11.1.1/FTOS-
SH-9.0.1.3.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!
Erasing Sseries ImageUpgrade Table of Contents, please wait
.!........................................................
..........................................................
..........................................................
..........................................................
..........................................................
..........................................................
..........................................................
..........................................................
..........................................................
....................................!
12946259 bytes successfully copied
FTOS#reload
```

54

Storm Control

The Dell Networking operating software (FTOS) storm control feature allows you to limit or suppress traffic during a traffic storm (Broadcast/Unknown Unicast Rate Limiting or Multicast).

The S5000 switch supports storm control.

Important Points to Remember

- Interface commands can only be applied on physical interfaces (virtual local area networks [VLANs] and link aggregation group [LAG] interfaces are not supported).
- An INTERFACE-level command only supports storm control configuration on ingress.
- An INTERFACE-level command overrides any CONFIGURATION-level ingress command for that physical interface, if both are configured.
- You can apply the CONFIGURATION-level storm control commands at ingress or egress and are supported on all physical interfaces.
- When storm control is applied on an interface, the percentage of storm control applied is calculated based on the advertised rate of the stack-unit. It is not based on the speed setting for the stack-unit.
- Do not apply per-VLAN quality of service (QoS) on an interface that has storm control enabled (either on an interface or globally).
- When you enable broadcast storm control on an interface or globally on ingress, and DSCP marking for a DSCP value 1 is configured for the data traffic, the traffic goes to queue 1 instead of queue 0.
- Similarly, if you enable unicast storm control on an interface or globally on ingress, and DSCP marking for a DSCP value 2 is configured for the data traffic, the traffic goes to queue 2 instead of queue 0.

NOTE: Bi-directional traffic (unknown unicast and broadcast) along with egress storm control causes the configured traffic rates to be split between the involved ports. The percentage of traffic that each port receives after the split is not predictable. These ports can be in the same/different port pipes or the same/different stack-units.

show storm-control broadcast

Display the storm control broadcast configuration.

S5000

Syntax `show storm-control broadcast [interface-type slot/port]`

Parameters

interface-type slot/port	(OPTIONAL) Enter one of the following keywords followed by slot/port information to display the interface specific storm control

configuration. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below.

- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show storm-control broadcast tengigabitethernet 3/24

Broadcast storm control configuration

Interface  Direction   Packets/Second
----------------------------------------
Te 3/24    Ingress     10000

FTOS#
```

show storm-control multicast

Display the storm control multicast configuration.

S5000

Syntax `show storm-control multicast [interface-type slot/port]`

Parameters

interface-type slot/port	(OPTIONAL) Enter one of the following keywords followed by slot/port information to display the interface specific storm control configuration. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

Defaults	none
Command Modes	- EXEC - EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
FTOS#show storm-control multicast tengigabitethernet 1/0

Multicast storm control configuration

Interface  Direction     Packets/Second
------------------------------------------
Te 1/0     Ingress       5

FTOS#
```

show storm-control unknown-unicast

Display the storm control unknown-unicast configuration.

S5000

Syntax `show storm-control unknown-unicast [interface-type slot/port]`

Parameters

interface-type slot/port	(OPTIONAL) Enter one of the following keywords followed by slot/port information to display the interface specific storm control configuration. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. - For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60.

Defaults	none
Command Modes	- EXEC - EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.

Example

```
FTOS#show storm-control unknown-unicast tengigabitethernet 3/0

Unknown-unicast storm control configuration

Interface  Direction  Packets/Second
--------------------------------------
Te 3/0     Ingress    1000

FTOS#
```

storm-control broadcast (Configuration)

Configure the percentage of broadcast traffic allowed in or out of the network.

S5000

Syntax

`storm-control broadcast [packets_per_second in]`

To disable broadcast rate-limiting, use the `no storm-control broadcast packets_per_second in]` command.

Parameters

***packets_per_second* in**	Enter the packets per second of broadcast traffic allowed into the network. The range is 0 to 33554431.

Defaults none

Command Modes CONFIGURATION (conf)

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Broadcast storm control is valid on Layer 2/Layer 3 interfaces only. Layer 2 broadcast traffic is treated as unknown-unicast traffic.

storm-control broadcast (Interface)

Configure the percentage of broadcast traffic allowed on an interface (ingress only).

S5000

Syntax

`storm-control broadcast [packets_per_second in]`

To disable broadcast storm control on the interface, use the `no storm-control broadcast [packets_per_second in]` command.

Parameters

***packets_per_second* in**	Enter the packets per second of broadcast traffic allowed into the network. The range is 0 to 33554431.

Defaults	none
Command Modes	INTERFACE (conf-if-*interface-slot/port*)
Command History	**Version 9.0(1.3)** Introduced on the S5000.

storm-control multicast (Configuration)

Configure the packets per second (pps) of multicast traffic allowed in to S5000 networks.

S5000

Syntax

`storm-control multicast packets_per_second in`

To disable storm-control for multicast traffic into the network, use the `no storm-control multicast packets_per_second in` command.

Parameters

packets_per_second in	Enter the packets per second of multicast traffic allowed into the network. The range is 0 to 33554431.

Defaults	none
Command Modes	CONFIGURATION (conf)
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	Broadcast traffic (all 0xFs) should be counted against the broadcast storm control meter, not against the multicast storm control meter. It is possible, however, that some multicast control traffic may get dropped when storm control thresholds are exceeded.

storm-control multicast (Interface)

Configure the percentage of multicast traffic allowed on an S5000 interface (ingress only) network only.

S5000

Syntax

`storm-control multicast packets_per_second in`

To disable multicast storm control on the interface, use the `no storm-control multicast packets_per_second in` command.

Parameters

packets_per_second in	Enter the packets per second of broadcast traffic allowed into the network. The range is 0 to 33554431.

Defaults	none
Command Modes	INTERFACE (conf-if-*interface-slot/port*)
Command History	**Version 9.0(1.3)** Introduced on the S5000.

storm-control unknown-unicast (Configuration)

Configure the percentage of unknown-unicast traffic allowed in or out of the network.

S5000

Syntax

`storm-control unknown-unicast [packets_per_second in]`

To disable storm control for unknown-unicast traffic, use the `no storm-control unknown-unicast [packets_per_second in]` command.

Parameters

packets_per_second in	Enter the packets per second of broadcast traffic allowed into the network. The range is 0 to 33554431.

Defaults none

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Unknown Unicast Storm-Control is valid for Layer 2 and Layer 2/Layer 3 interfaces.

storm-control unknown-unicast (Interface)

Configure percentage of unknown-unicast traffic allowed on an interface (ingress only).

S5000

Syntax

`storm-control unknown-unicast [packets_per_second in]`

To disable unknown-unicast storm control on the interface, use the `no storm-control unknown-unicast [packets_per_second in]` command.

Parameters

packets_per_second in	Enter the packets per second of broadcast traffic allowed into the network. The range is 0 to 33554431.

Defaults none

Command Modes	INTERFACE (conf-if-*interface-slot/port*)
Command History	

Version 9.0(1.3)	Introduced on the S5000.

55

System Time and Date

The commands in this chapter configure time values on the system, either using the Dell Networking operating software (FTOS), or the hardware, or using the network time protocol (NTP). With NTP, the switch can act only as a client to an NTP clock host.

For more information, refer to the “Network Time Protocol” section of the *Management* chapter in the *FTOS Configuration Guide*.

calendar set

Set the time and date for the switch hardware clock.

S5000

Syntax `calendar set time month day year`

Parameters

time	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format; for example, 17:15:00 is 5:15 pm.
month	Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to time day month year.
day	Enter the number of the day. The range is 1 to 31. You can enter the name of a month to change the order of the display to time day month year.
year	Enter a four-digit number as the year. The range is 1993 to 2035.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can change the order of the month and day parameters to enter the time and date as time day month year.

In the switch, the hardware clock is separate from the software and is called the calendar. This hardware clock runs continuously. After the hardware clock (the calendar) is set, the FTOS automatically updates the software clock after system bootup. You cannot delete the hardware clock (calendar).

To manually update the software with the hardware clock, use the `clock read-calendar` command.

Example

```
FTOS#calendar set 08:55:00 june 18 2006
FTOS#
```

Related Commands

clock read-calendar – sets the software clock based on the hardware clock.

clock set – sets the software clock.

clock update-calendar – sets the hardware clock based on the software clock.

show clock – displays the clock settings.

clock read-calendar

Set the software clock on the switch from the information set in hardware clock (calendar).

S5000

Syntax `clock read-calendar`

Defaults Not configured.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

In the switch, the hardware clock is separate from the software and is called the calendar. This hardware clock runs continuously. After the hardware clock (the calendar) is set, the FTOS automatically updates the software clock after system bootup.

You cannot delete this command (there is not a `no` version of this command).

clock set

Set the software clock in the switch.

S5000

Syntax `clock set` *`time month day year`*

Parameters

time	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format; example, 17:15:00 is 5:15 pm.
month	Enter the name of one of the 12 months, in English. You can enter the number of a day and change the order of the display to time day month year.
day	Enter the number of the day. The range is 1 to 31. You can enter the name of a month to change the order of the display to time month day year.

year	Enter a four-digit number as the year. The range is 1993 to 2035.

Defaults

Not configured.

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can change the order of the `month` and `day` parameters to enter the time and date as time day month year. You cannot delete the software clock.

The software clock runs only when the software is up. The clock restarts, based on the hardware clock, when the switch reboots.

Dell Networking recommends using an outside time source, such as NTP, to ensure accurate time on the switch.

Example

```
FTOS#clock set 16:20:00 19 may 2001
FTOS#
```

Related Commands

ntp update-calendar – sets the switch using the NTP settings.

clock summer-time date

Set a date (and time zone) on which to convert the switch to daylight saving time on a one-time basis.

S5000

Syntax

```
clock summer-time time-zone date start-month start-day start-
year start-time end-month end-day end-year end-time [offset]
```

To delete a daylight saving time zone configuration, use the `no clock summer-time` command.

Parameters

time-zone	Enter the three-letter name for the time zone. This name is displayed in the show clock output.
start-month	Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to time day month year.
start-day	Enter the number of the day. The range is 1 to 31. You can enter the name of a month to change the order of the display to time day month year.
start-year	Enter a four-digit number as the year. The range is 1993 to 2035.
start-time	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.

end-day	Enter the number of the day. The range is 1 to 31. You can enter the name of a month to change the order of the display to time day month year.
end-month	Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to time day month year.
end-time	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
end-year	Enter a four-digit number as the year. The range is 1993 to 2035.
offset	(OPTIONAL) Enter the number of minutes to add during the summer-time period. The range is 1 to1440. The default is **60 minutes**.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

calendar set – sets the hardware clock.

clock summer-time recurring – sets a date (and time zone) on which to convert the switch to daylight saving time each year.

show clock – displays the current clock settings.

clock summer-time recurring

Set the software clock to convert to daylight saving time on a specific day each year.

S5000

Syntax

```
clock summer-time time-zone recurring [start-week start-day
start-month start-time end-week end-day end-month end-time
[offset]]
```

To delete a daylight saving time zone configuration, use the `no clock summer-time` command.

Parameters

time-zone	Enter the three-letter name for the time zone. This name is displayed in the show clock output. You can enter up to eight characters.
start-week	(OPTIONAL) Enter one of the following as the week that daylight saving begins and then enter values for start-day through end-time: • `week-number`: Enter a number from 1 to 4 as the number of the week in the month to start daylight saving time. • `first`: Enter this keyword to start daylight saving time in the first week of the month.

	- `last`: Enter this keyword to start daylight saving time in the last week of the month.
start-day	Enter the name of the day that you want daylight saving time to begin. Use English three letter abbreviations; for example, Sun, Sat, Mon, etc. The range is Sun to Sat.
start-month	Enter the name of one of the 12 months in English.
start-time	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
end-week	Enter the one of the following as the week that daylight saving ends: - `week-number`: enter a number from 1 to 4 as the number of the week to end daylight saving time. - `first`: enter the keyword `first` to end daylight saving time in the first week of the month. - `last`: enter the keyword `last` to end daylight saving time in the last week of the month.
end-day	Enter the weekday name that you want daylight saving time to end. Enter the weekdays using the three letter abbreviations; for example Sun, Sat, Mon etc. The range is Sun to Sat.
end-month	Enter the name of one of the 12 months in English.
end-time	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format; example, 17:15:00 is 5:15 pm.
offset	(OPTIONAL) Enter the number of minutes to add during the summer-time period. The range is 1 to 1440. The default is **60 minutes**.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

calendar set – sets the hardware clock.

clock summer-time date – sets a date (and time zone) on which to convert the switch to daylight saving time on a one-time basis.

show clock – displays the current clock settings.

clock timezone

Configure a timezone for the switch.

S5000

Syntax

```
clock timezone timezone-name offset
```

To delete a timezone configuration, use the `no clock timezone` command.

Parameters

timezone-name	Enter the name of the timezone. You cannot use spaces.
offset	Enter one of the following: • a number from 1 to 23 as the number of hours in addition to universal time coordinated (UTC) for the timezone. • a minus sign (-) followed by a number from 1 to 23 as the number of hours.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Coordinated universal time (UTC) is the time standard based on the International Atomic Time standard, commonly known as Greenwich Mean time. When determining system time, you must include the differentiator between UTC and your local timezone. For example, San Jose, CA is the Pacific Timezone with a UTC offset of -8.

clock update-calendar

Set the switch hardware clock based on the software clock.

S5000

Syntax

```
clock update-calendar
```

Defaults Not configured.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Use this command only if you are sure that the hardware clock is inaccurate and the software clock is correct. You cannot delete this command (there is not a `no` form of this command).

Related Commands calendar set – sets the hardware clock.

debug ntp

Display network time protocol (NTP) transactions and protocol messages for troubleshooting.

S5000

Syntax

`debug ntp {adjust | all | authentication | events | loopfilter | packets | select | sync}`

To disable debugging of NTP transactions, use the `no debug ntp {adjust | all | authentication | events | loopfilter | packets | select | sync}` command.

Parameters

adjust	Enter the keyword `adjust` to display information on NTP clock adjustments.
all	Enter the keyword `all` to display information on all NTP transactions.
authentication	Enter the keyword `authentication` to display information on NTP authentication transactions.
events	Enter the keyword `events` to display information on NTP events.
loopfilter	Enter the keyword `loopfilter` to display information on NTP local clock frequency.
packets	Enter the keyword `packets` to display information on NTP packets.
select	Enter the keyword `select` to display information on the NTP clock selection.
sync	Enter the keyword `sync` to display information on the NTP clock synchronization.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

ntp authenticate

Enable authentication of NTP traffic between the switch and the NTP time serving hosts.

S5000

Syntax

`ntp authenticate`

To disable NTP authentication, use the `no ntp authentication` command.

Defaults Not enabled.

Command Modes CONFIGURATION

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You also must configure an authentication key for NTP traffic using the `ntp authentication-key` command.

Related Commands

ntp authentication-key – configures the authentication key for NTP traffic.

ntp trusted-key – configures a key to authenticate.

ntp authentication-key

Specify a key for authenticating the NTP server.

S5000

Syntax

```
ntp authentication-key number md5 [0 | 7] key
```

Parameters

number	Specify a number for the authentication key. The range is 1 to 4294967295. This number must be the same as the `number` parameter configured in the `ntp trusted-key` command.
md5	Specify that the authentication key is encrypted using MD5 encryption algorithm.
0	Specify that authentication key is entered in an unencrypted format (default).
7	Specify that the authentication key is entered in DES encrypted format.
key	Enter the authentication key in the previously specified format.

Defaults

NTP authentication is not configured by default. If you do not specify the option [`0` | `7`], **0** is selected by default.

Command Modes

CONFIGURATION

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Usage Information

After configuring the `ntp authentication-key` command, configure the `ntp trusted-key` command to complete NTP authentication.

FTOS uses DES encryption to store the key in the startup-config when you enter the `ntp authentication-key` command.

Related Commands

ntp authenticate – enables NTP authentication.

ntp trusted-key – configures a trusted key.

ntp broadcast client

Set up the interface to receive NTP broadcasts from an NTP server.

S5000

Syntax	`ntp broadcast client` To disable broadcast, use the `no ntp broadcast client` command.
Defaults	Disabled.
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ntp disable

Prevent an interface from receiving NTP packets.

S5000

Syntax	`ntp disable` To re-enable NTP on an interface, use the `no ntp disable` command.
Defaults	Disabled (that is, if you configure an NTP host, all interfaces receive NTP packets)
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ntp multicast client

Configure the switch to receive NTP information from the network via multicast.

S5000

Syntax	`ntp multicast client [`*`multicast-address`*`]` To disable multicast reception, use the `no ntp multicast client [`*`multicast-address`*`]` command.
Parameters	***multicast-address*** (OPTIONAL) Enter a multicast address. Enter either an IPv4 address in dotted decimal format or an IPv6 address in X:X:X:X::X format. If you do not enter a multicast address, the address:

- 224.0.1.1 is configured if the interface address is IPv4
- ff05::101 is configured if the interface address is IPv6

Defaults	Not configured.
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** Introduced on the S5000.

ntp server

Configure an NTP time-serving host.

S5000

Syntax

`ntp server {hostname | ipv4-address | ipv6-address} [key keyid] [prefer] [version number]`

Parameters

ipv4-address | *ipv6-address*	Enter an IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X).
hostname	Enter the hostname of the server.
key *keyid*	(OPTIONAL) Enter the keyword `key` and a number as the NTP peer key. The range is 1 to 4294967295.
prefer	(OPTIONAL) Enter the keyword `prefer` to indicate that this peer has priority over other servers.
version *number*	(OPTIONAL) Enter the keyword `version` and a number to correspond to the NTP version used on the server. The range is 1 to 3.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can configure multiple time serving hosts (up to 250). From these time serving hosts, the FTOS choses one NTP host with which to synchronize. Use the `show ntp associations` command to determine which server was selected.

Because a large number of polls to NTP hosts can impact network performance, Dell Networking recommends limiting the number of hosts configured.

Related Commands

show ntp associations – displays the NTP servers configured and their status.

ntp source

Specify an interface's IP address to be included in the NTP packets.

S5000

Syntax `ntp source interface-type slot/port`

To delete the configuration, use the `no ntp source` command.

Parameters

interface-type slot/port	Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

ntp trusted-key

Set a key to authenticate the system to which NTP will synchronize.

S5000

Syntax `ntp trusted-key number`

To delete the key, use the `no ntp trusted-key number` command.

Parameters

number	Enter a number as the trusted key ID. The range is 1 to 4294967295.

Defaults Not configured.

Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Usage Information	The `number` parameter in the `ntp trusted-key` command must be the same number as the `number` parameter in the `ntp authentication-key` command. If you change the `ntp authentication-key` command, you must also change the `ntp trusted-key` command.
Related Commands	ntp authentication-key – sets an authentication key for NTP. ntp authenticate – enables the NTP authentication parameters you set.

ntp update-calendar

Configure the FTOS to update the calendar (the hardware clock) with the NTP-derived time.

S5000

Syntax	`ntp update-calendar [`*`minutes`*`]` To return to default setting, use the `no ntp update-calendar` command.
Parameters	*minutes* (OPTIONAL) Enter the number of minutes between updates from NTP to the hardware clock. The range is 1 to 1440. The default is **60 minutes**.
Defaults	Not enabled.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** Introduced on the S5000.

show calendar

Display the current date and time based on the switch hardware clock.

S5000

Syntax

```
show calendar
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show calendar
16:33:30 UTC Tue Jun 26 2001
FTOS#
```

Related Commands

show clock – displays the time and date from the switch software clock.

show clock

Display the current clock settings.

S5000

Syntax

```
show clock [detail]
```

Parameters

detail	(OPTIONAL) Enter the keyword `detail` to view the source information of the clock.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show clock
11:05:56.949 UTC Thu Oct 25 2001
FTOS#
```

Example (Detail)

```
FTOS#show clock detail
12:18:10.691 UTC Wed Jan 7 2009
Time source is RTC hardware
Summer time starts 02:00:00 UTC Sun Mar 8 2009
Summer time ends 02:00:00 ABC Sun Nov 1 2009
FTOS#
```

Related Commands

clock summer-time recurring – displays the time and date from the switch hardware clock.

show calendar – displays the time and date from the switch hardware clock.

show ntp associations

Display the NTP master and peers.

S5000

Syntax `show ntp associations`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ntp associations` command shown in the Example below.

Field	Description
(none)	One or more of the following symbols could be displayed: • * means synchronized to this peer. • # means almost synchronized to this peer. • + means the peer was selected for possible synchronization. • - means the peer is a candidate for selection. • ~ means the peer is statically configured.
remote	Displays the remote IP address of the NTP peer.
ref clock	Displays the IP address of the remote peer's reference clock.
st	Displays the peer's stratum, that is, the number of hops away from the external time source. A 16 in this column means the NTP peer cannot reach the time source.
when	Displays the last time the switch received an NTP packet.
poll	Displays the polling interval (in seconds).
reach	Displays the reachability to the peer (in octal bitstream).
delay	Displays the time interval or delay for a packet to complete a round-trip to the NTP time source (in milliseconds).
offset	Displays the relative time of the NTP peer's clock to the switch clock (in milliseconds).
disp	Displays the dispersion.

Example

```
FTOS#show ntp associations
remote      ref clock  st when poll reach delay  offset disp
=============================================================
 10.10.120.5 0.0.0.0     16 - 256        0 0.00 0.000 16000.0
*172.16.1.33 127.127.1.0 11 6 16         377   -0.08 -1499.9
104.16
 172.31.1.33 0.0.0.0     16 - 256        0 0.00 0.000 16000.0
 192.200.0.2 0.0.0.0     16 - 256        0 0.00 0.000 16000.0
* master (synced), # master (unsynced), + selected, - candidate
FTOS#
```

Related Commands

show ntp status – displays the current NTP status.

show ntp status

Display the current NTP status.

S5000

Syntax

```
show ntp status
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes the `show ntp status` command shown in the Example below.

Field	Description
Clock is...	States whether or not the switch clock is synchronized, which NTP stratum the system is assigned and the IP address of the NTP peer.
frequency is...	Displays the frequency (in ppm), stability (in ppm) and precision (in Hertz) of the clock in this system.
reference time is...	Displays the reference time stamp.
clock offset is...	Displays the system offset to the synchronized peer and the time delay on the path to the NTP root clock.
root dispersion is...	Displays the root and path dispersion.
peer mode is...	State what NTP mode the switch is. This should be Client mode.

Example

```
FTOS#sh ntp status
Clock is synchronized, stratum 2, reference is 100.10.10.10
frequency is -32.000 ppm, stability is 15.156 ppm, precision
is 4294967290
reference time is BC242FD5.C7C5C000 (10:15:49.780 UTC Mon Jan
10 2000)
clock offset is clock offset msec, root delay is 0.01656 sec
root dispersion is 0.39694 sec, peer dispersion is peer
dispersion msec
peer mode is client
FTOS#
```

Related Commands	show ntp associations – displays information on the NTP master and peer configurations.

56

Uplink Failure Detection (UFD)

Uplink failure detection (UFD) provides detection of the loss of upstream connectivity and, if used with NIC teaming, automatic recovery from a failed link. UFD is supported on the S5000 switch.

clear ufd-disable

Re-enable one or more downstream interfaces on the switch/router that are in a UFD-Disabled Error state so that an interface can send and receive traffic.

S5000

Syntax

```
clear ufd-disable {interface type slot/port | uplink-state-group group-id}
```

Parameters

interface *type slot/port*	Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: `gigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.
uplink-state-group *group-id*	Re-enables all UFD-disabled downstream interfaces in the group. The valid group-id values are 1 to 16.

Defaults

A downstream interface in an uplink-state group that has been disabled by UFD is disabled and in a UFD-Disabled Error state.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

- downstream – assigns a port or port-channel to the uplink-state group as a downstream interface.

- uplink-state-group – creates an uplink-state group and enables the tracking of upstream links.

debug uplink-state-group

Enable debug messages for events related to a specified uplink-state group or all groups.

S5000

Syntax

```
debug uplink-state-group [group-id]
```

To turn off debugging event messages, enter the `no debug uplink-state-group [group-id]` command.

Parameters

group-id	Enables debugging on the specified uplink-state group. The valid group-id values are 1 to 16.

Defaults

none

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

clear ufd-disable – re-enables downstream interfaces that are in a UFD-Disabled Error state.

description

Enter a text description of an uplink-state group.

S5000

Syntax

```
description text
```

Parameters

text	Text description of the uplink-state group. The maximum length is 80 alphanumeric characters.

Defaults

none

Command Modes

UPLINK-STATE-GROUP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-uplink-state-group-16)# description test
FTOS(conf-uplink-state-group-16)#
```

Related Commands	uplink-state-group – creates an uplink-state group and enables the tracking of upstream links.

downstream

Assign a port or port-channel to the uplink-state group as a downstream interface.

S5000

Syntax

`downstream` *`interface-type slot/port`*

To delete an uplink-state group, enter the `no downstream interface` command.

Parameters

interface-type slot/port	Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: `tengigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.

Defaults

none

Command Modes

UPLINK-STATE-GROUP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can assign physical port or port-channel interfaces to an uplink-state group.

You can assign an interface to only one uplink-state group. You must configure each interface assigned to an uplink-state group as either an upstream or downstream interface, but not both.

You can assign individual member ports of a port channel to the group. An uplink-state group can contain either the member ports of a port channel or the port channel itself, but not both.

Related Commands

- upstream – assigns a port or port-channel to the uplink-state group as an upstream interface.

- uplink-state-group – creates an uplink-state group and enables the tracking of upstream links.

downstream auto-recover

Enable auto-recovery so that UFD-disabled downstream ports in an uplink-state group automatically come up when a disabled upstream port in the group comes back up.

S5000

Syntax	`downstream auto-recover` To disable auto-recovery on downstream links, use the `no downstream auto-recover` command.
Defaults	The auto-recovery of UFD-disabled downstream ports is enabled.
Command Modes	UPLINK-STATE-GROUP
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	• downstream – assigns a port or port-channel to the uplink-state group as a downstream interface. • uplink-state-group – creates an uplink-state group and enables the tracking of upstream links.

downstream disable links

Configure the number of downstream links in the uplink-state group that will be disabled if one upstream link in an uplink-state group goes down.

S5000

Syntax	`downstream disable links {number |all}` To revert to the default setting, use the `no downstream disable links` command.

Parameters

number	Enter the number of downstream links to be brought down by UFD. The range is 1 to 1024.
all	Brings down all downstream links in the group.

Defaults	No downstream links are disabled when an upstream link in an uplink-state group goes down.
Command Modes	UPLINK-STATE-GROUP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

A user-configurable number of downstream interfaces in an uplink-state group are put into a link-down state with an UFD-Disabled error message when one upstream interface in an uplink-state group goes down.

If all upstream interfaces in an uplink-state group go down, all downstream interfaces in the same uplink-state group are put into a link-down state.

Related Commands

- downstream – assigns a port or port-channel to the uplink-state group as a downstream interface.
- uplink-state-group – creates an uplink-state group and enables the tracking of upstream links.

enable

Enable uplink state group tracking for a specific UFD group.

S5000

Syntax

`enable`

To disable upstream-link tracking without deleting the uplink-state group, use the `no enable` command.

Defaults

Upstream-link tracking is automatically enabled in an uplink-state group.

Command Modes

UPLINK-STATE-GROUP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands

- uplink-state-group – creates an uplink-state group and enables the tracking of upstream links.

show running-config uplink-state-group

Display the current configuration of one or more uplink-state groups.

S5000

Syntax

`show running-config uplink-state-group [`*`group-id`*`]`

Parameters

group-id	Displays the current configuration of all uplink-state groups or a specified group. The valid group-id values are 1 to 16.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show running-config uplink-state-group
!
no enable
uplink state track 1
downstream GigabitEthernet 0/2,4,6,11-19
upstream TengigabitEthernet 0/48, 52
upstream PortChannel 1
!
uplink state track 2
downstream GigabitEthernet 0/1,3,5,7-10
upstream TengigabitEthernet 0/56,60
```

Related Commands

- show uplink-state-group – displays the status information on a specified uplink-state group or all groups.
- uplink-state-group – creates an uplink-state group and enables the tracking of upstream links.

show uplink-state-group

Display status information on a specified uplink-state group or all groups.

S5000

Syntax `show uplink-state-group [group-id] [detail]`

Parameters

group-id	Displays status information on a specified uplink-state group or all groups. The valid group-id values are 1 to 16.
detail	Displays additional status information on the upstream and downstream interfaces in each group

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS# show uplink-state-group
Uplink State Group: 1 Status: Enabled, Up
Uplink State Group: 3 Status: Enabled, Up
Uplink State Group: 5 Status: Enabled, Down
Uplink State Group: 6 Status: Enabled, Up
Uplink State Group: 7 Status: Enabled, Up
Uplink State Group: 16 Status: Disabled, Up

FTOS# show uplink-state-group 16
Uplink State Group: 16 Status: Disabled, Up

FTOS#show uplink-state-group detail
(Up): Interface up (Dwn): Interface down (Dis): Interface
disabled
Uplink State Group    : 1 Status: Enabled, Up
Upstream Interfaces   :
Downstream Interfaces :

Uplink State Group    : 3 Status: Enabled, Up
Upstream Interfaces   : Gi 0/46(Up) Gi 0/47(Up)
Downstream Interfaces : Te 13/0(Up) Te 13/1(Up) Te 13/3(Up) Te
13/5(Up) Te 13/6(Up)

Uplink State Group    : 5 Status: Enabled, Down
Upstream Interfaces   : Gi 0/0(Dwn) Gi 0/3(Dwn) Gi 0/5(Dwn)
Downstream Interfaces : Te 13/2(Dis) Te 13/4(Dis) Te
13/11(Dis) Te 13/12(Dis) Te 13/13(Dis) Te 13/14(Dis) Te
13/15(Dis)

Uplink State Group    : 6 Status: Enabled, Up
Upstream Interfaces   :
Downstream Interfaces :

Uplink State Group    : 7 Status: Enabled, Up
Upstream Interfaces   :
Downstream Interfaces :

Uplink State Group    : 16 Status: Disabled, Up
Upstream Interfaces   : Te 0/41(Dwn) Po 8(Dwn)
Downstream Interfaces : Te 0/40(Dwn)
```

Related Commands

- show running-config uplink-state-group – displays the current configuration of one or more uplink-state groups.
- uplink-state-group – create an uplink-state group and enables the tracking of upstream links.

uplink-state-group

Create an uplink-state group and enable the tracking of upstream links on a switch/ router.

S5000

Syntax

`uplink-state-group group-id`

To delete an uplink-state group, enter the `no uplink-state-group group-id` command.

Parameters

group-id	Enter the ID number of an uplink-state group. The range is 1 to 16.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

After you enter the command, enter Uplink-State-Group Configuration mode to assign upstream and downstream interfaces to the group.

An uplink-state group is considered to be operationally up if at least one upstream interface in the group is in the Link-Up state.

An uplink-state group is considered to be operationally down if no upstream interfaces in the group are in the Link-Up state. No uplink-state tracking is performed when a group is disabled or in an operationally down state.

To disable upstream-link tracking without deleting the uplink-state group, use the `no enable` command in uplink-state-group configuration mode.

Example

```
FTOS(conf)#uplink-state-group 16
FTOS(conf-uplink-state-group-16)#
02:23:17: %STKUNIT0-M:CP %IFMGR-5-ASTATE_UP: Changed uplink
state group Admin state to up: Group 16
```

Related Commands

- show running-config uplink-state-group – displays the current configuration of one or more uplink-state groups.
- show uplink-state-group – displays the status information on a specified uplink-state group or all groups.

upstream

Assign a port or port-channel to the uplink-state group as an upstream interface.

S5000

Syntax

`upstream interface-type slot/port`

To delete an uplink-state group, use the `no upstream interface` command.

Parameters

interface-type slot/port	Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: `tengigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.

Defaults none

Command Modes UPLINK-STATE-GROUP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You can assign physical port or port-channel interfaces to an uplink-state group.

You can assign an interface to only one uplink-state group. You must configure each interface assigned to an uplink-state group as either an upstream or downstream interface, but not both.

You can assign individual member ports of a port channel to the group. An uplink-state group can contain either the member ports of a port channel or the port channel itself, but not both.

Example

```
FTOS(conf-uplink-state-group-16)# upstream tengigabitethernet
1/10-15
FTOS(conf-uplink-state-group-16)#
```

Related Commands

- downstream – assigns a port or port-channel to the uplink-state group as a downstream interface.
- uplink-state-group – creates an uplink-state group and enables the tracking of upstream links.

57

VLAN Stacking

With the virtual local area network (VLAN)-stacking feature (also called stackable VLANs and QinQ), you can “stack” VLANs into one tunnel and switch them through the network transparently.

This feature is supported by the Dell Networking operating software (FTOS) on the S5000.

For more information about basic VLAN commands, refer to the *Virtual LAN (VLAN) Commands* section in the Layer 2 chapter.

Important Points to Remember

- If you do not enable the spanning tree protocol (STP) across the stackable VLAN network, STP bridge protocol data units (BPDUs) from the customer’s networks are tunneled across the stackable VLAN network.
- If you do enable STP across the stackable VLAN network, STP BPDUs from the customer’s networks are consumed and not tunneled across the stackable VLAN network unless you enable protocol tunneling.
- Layer 3 protocols are not supported on a stackable VLAN network.
- Assigning an IP address to a stackable VLAN is supported when all the members are only stackable VLAN trunk ports. IP addresses on a stackable VLAN-enabled VLAN is not supported if the VLAN contains stackable VLAN access ports. This facility is provided for the simple network management protocol (SNMP) management over a stackable VLAN-enabled VLAN containing only stackable VLAN trunk interfaces. Layer 3 routing protocols on such a VLAN are not supported.
- Dell Networking recommends that you do not use the same MAC address, on different customer VLANs, on the same stackable VLAN.
- Interfaces configured using stackable VLAN access or stackable VLAN trunk commands are not switch traffic for the default VLAN. These interfaces are switch traffic only when they are added to a non-default VLAN.
- A vlan-stack trunk port is also allowed to be configured as a tagged port and as an untagged port for single-tagged VLANs. When the vlan-stack trunk port is also a member of an untagged vlan, the port must be in Hybrid mode. Refer to portmode hybrid.

dei enable

Make packets eligible for dropping based on their DEI value.

S5000

Syntax	`dei enable`
Defaults	Packets are colored green; no packets are dropped.
Command Modes	CONFIGURATION

Command History	**Version 9.0(1.3)**	Introduced on the S5000.

dei honor

Honor the incoming DEI value by mapping it to an FTOS drop precedence. You may enter the command once for 0 and once for 1.

S5000

Syntax `dei honor {0 | 1} {green | red | yellow}`

Parameters

0 | 1	Enter the bit value you want to map to a color.
green | red | yellow	Choose a color: • `Green`: High priority packets that are the least preferred to be dropped. • `Yellow`: Lower priority packets that are treated as best-effort. • `Red`: Lowest priority packets that are always dropped (regardless of congestion status).

Defaults	Disabled; Packets with an unmapped DEI value are colored green.	
Command Modes	INTERFACE	
Command History	**Version 9.0(1.3)**	Introduced on the S5000.
Usage Information	You must first enable DEI for this configuration to take effect.	
Related Commands	dei enable – enables DEI.	

dei mark

Set the DEI value on egress according to the color currently assigned to the packet.

S5000

Syntax `dei mark {green | yellow} {0 | 1}`

Parameters

0 | 1	Enter the bit value you want to map to a color.

green | red | yellow	Choose a color: • `Green`: High priority packets that are the least preferred to be dropped. • `Yellow`: Lower priority packets that are treated as best-effort.

Defaults All the packets on egress are marked with DEI 0.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information You must first enable DEI for this configuration to take effect.

Related Commands dei enable – enables DEI.

member

Assign a stackable VLAN access or trunk port to a VLAN. The VLAN must contain the `vlan-stack compatible` command in its configuration.

S5000

Syntax `member` *`interface-type slot/port`*

To remove an interface from a Stackable VLAN, use the `no member` *`interface-type slot/port`* command.

Parameters

interface-type slot/port	Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.

Defaults Not configured.

Command Modes CONF-IF-VLAN

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Usage Information You must enable the stackable VLAN (using the `vlan-stack compatible` command) on the VLAN prior to adding a member to the VLAN.

Related Commands vlan-stack compatible – enables stackable VLAN on a VLAN.

show interfaces dei-honor

Display the dei honor configuration.

S5000

Syntax `show interfaces dei-honor [interface-type slot/port | stack–unit unit-number port-set number]`

Parameters

interface-type slot/port	Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
stack-unit *unit-number* **port-set** *number*	Enter the keywords `stack-unit` followed by the unit number. The range is 0 to 11. Then enter the keywords `port-set` followed by the port-pipe number.

Command Modes EXEC Privilege

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show interfaces dei-honor

Default Drop precedence: Green
Interface   CFI/DEI          Drop precedence
---------------------------------------------
Te 0/1      0                Green
Te 0/1      1                Yellow
Te 8/9      1                Red
Te 8/40     0                Yellow
```

Related Commands dei honor

show interfaces dei-mark

Display the dei mark configuration.

S5000

Syntax `show interfaces dei-mark [interfacetype slot/port | stack—unit unit-number port-set number]`

Parameters

interface-type slot/port	Enter the `interface` keyword followed by the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128.
stack-unit ***unit-number*** **port-set** ***number***	Enter the keyword `stack-unit` followed by the unit number. The range is 0 to 11. Then enter the keyword `port-set` followed by the port-pipe number.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show interfaces dei-mark

Default CFI/DEI Marking: 0
Interface   Drop precedence      CFI/DEI
------------------------------------------------
Te 0/1      Green                0
Te 0/1      Yellow               1
Te 8/9      Yellow               0
Te 8/40     Yellow               0
```

Related Commands dei mark

stack-unit stack-group

Configure stacking group specified by ID.

S5000

Syntax `[no] stack-unit unit-number stack-group stack-group-number`

Parameters

unit-number	Enter the stack unit number. The range is 0 to 11..
stack-group-id	Enter the stack group number. The range is 0 to 15.
[no]	Use `no stack-unit unit-id stack-group stack-id` to remove the current stack group configuration.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

⚠ **WARNING: The following message displays to confirm the command: `All non-default configurations on the related member ports ports (<ports listed here>) will be removed. Do you want to continue (y/n)?` If you enter "y", all non-default configurations on any member ports of the current stack group is removed when the unit is rebooted.**

vlan-stack access

Specify a Layer 2 port or port channel as an access port to the stackable VLAN network.

S5000

Syntax `vlan-stack access`

To remove access port designation, use the `no vlan-stack access` command.

Defaults Not configured.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Prior to enabling this command, you must enter the `switchport` command to place the interface in Layer 2 mode.

To remove the access port designation, the port must be removed (using the `no member interface` command) from all stackable VLAN enabled VLANs.

vlan-stack compatible

Enable the stackable VLAN feature on a VLAN.

S5000

Syntax

`vlan-stack compatible`

To disable the Stackable VLAN feature on a VLAN, use the `no vlan-stack compatible` command.

Defaults

Not configured.

Command Modes

CONF-IF-VLAN

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You must remove the members prior to disabling the stackable VLAN feature.

To view the stackable VLANs, use the `show vlan` command in EXEC Privilege mode. Stackable VLANs contain members, designated by the M in the Q column of the command output.

Example

```
FTOS#show vlan

Codes: * - Default VLAN, G - GVRP VLANs

   NUM  Status    Q Ports
*  1    Inactive
   2    Active    M Te 13/13
                  M Te 13/0-2
   3    Active    M Po1(Te 13/14-15)
                  M Te 13/18
                  M Te 13/3
   4    Active    M Po1(Te 13/14-15)
                  M Te 13/18
                  M Te 13/4
   5    Active    M Po1(Te 13/14-15)
                  M Te 13/18
                  M Te 13/5
FTOS#
```

vlan-stack dot1p-mapping

Map C-Tag dot1p values to a S-Tag dot1p value. C-Tag values may be separated by commas and dashed ranges are permitted. Dynamic mode CoS overrides any Layer 2 QoS configuration in case of conflicts.

S5000

Syntax

`vlan-stack dot1p-mapping c-tag-dot1p` *`values`* `sp-tag-dot1p` *`value`*

Parameters

c-tag-dot1p ***value***	Enter the keyword `c-tag-dot1p` followed by the customer dot1p value that will be mapped to a service provider do1p value. The range is 0 to 7.
sp-tag-dot1p ***value***	Enter the keyword `sp-tag-dot1p` followed by the service provider dot1p value. The range is 0 to 7.

Defaults none

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

vlan-stack protocol-type

Define the stackable VLAN tag protocol identifier (TPID) for the outer VLAN tag (also called the VMAN tag). If you do not configure this command, FTOS assigns the value 0x9100.

S5000

Syntax `vlan-stack protocol-type number`

Parameters

number	Enter the hexadecimal number as the stackable VLAN tag. You may specify both bytes of the 2-byte S-Tag TPID. The range is 0 to FFFF. The default is **9100**.

Defaults 0x9100

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

For specific interoperability limitations regarding the S-Tag TPID, refer to the *FTOS Configuration Guide*.

The four characters you enter in the CLI for number are interpreted, as shown below:

1	0x0001
10	0x0010
81	0x0081
8100	0x8100

Related Commands

portmode hybrid – sets a port (physical ports only) to accept both tagged and untagged frames. A port configured this way is identified as a hybrid port in report displays.

vlan-stack trunk – specifies a Layer 2 port or port channel as a trunk port to the Stackable VLAN network.

vlan-stack trunk

Specify a Layer 2 port or port channel as a trunk port to the Stackable VLAN network.

S5000

Syntax

`vlan-stack trunk`

To remove a trunk port designation from the selected interface, use the `no vlan-stack trunk` command.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Prior to using this command, you must execute the `switchport` command to place the interface in Layer 2 mode.

To remove the trunk port designation, the port must first be removed (using the `no member interface` command) from all stackable VLAN-enabled VLANs.

A VLAN-Stack trunk port is also allowed to be configured as a tagged port and as an untagged port for single-tagged VLANs. When the VLAN-Stack trunk port is also a member of an untagged VLAN, the port must be in Hybrid mode. Refer to portmode hybrid.

In Example 1 below, a VLAN-Stack trunk port is configured and then also made part of a single-tagged VLAN.

In Example 2 below, the tag protocol identifier (TPID) is set to 8848. The “Gi 3/10” port is configured to act as a VLAN-Stack access port, while the “TenGi 8/0” port acts as a VLAN-Stack trunk port, switching stackable VLAN traffic for VLAN 10, while also switching untagged traffic for VLAN 30 and tagged traffic for VLAN 40. (To allow VLAN 30 traffic, the native VLAN feature is required, by executing the `portmode hybrid` command. Refer to portmode hybrid in Interfaces.

Example 1

```
FTOS(conf-if-gi-0/42)#switchport
FTOS(conf-if-gi-0/42)#vlan-stack trunk
FTOS(conf-if-gi-0/42)#show config
!
interface GigabitEthernet 0/42
  no ip address
  switchport
  vlan-stack trunk
  no shutdown
FTOS(conf-if-gi-0/42)#interface vlan 100
FTOS(conf-if-vl-100)#vlan-stack compatible
FTOS(conf-if-vl-100-stack)#member gigabitethernet 0/42
FTOS(conf-if-vl-100-stack)#show config
!
interface Vlan 100
```

```
  no ip address
  vlan-stack compatible
  member GigabitEthernet 0/42
  shutdown
FTOS(conf-if-vl-100-stack)#interface vlan 20
FTOS(conf-if-vl-20)#tagged gigabitethernet 0/42
FTOS(conf-if-vl-20)#show config
!
interface Vlan 20
  no ip address
  tagged GigabitEthernet 0/42
  shutdown
FTOS(conf-if-vl-20)#do show vlan
Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack

  NUM  Status Description   Q Ports
* 1    Inactive
  20   Active               T Gi 0/42
  100  Active               M Gi 0/42
FTOS(conf-if-vl-20)#
```

Example 2

```
FTOS(config)#vlan-stack protocol-type 88A8
FTOS(config)#interface gigabitethernet 3/10
FTOS(conf-if-gi-3/10)#no shutdown
FTOS(conf-if-gi-3/10)#switchport
FTOS(conf-if-gi-3/10)#vlan-stack access
FTOS(conf-if-gi-3/10)#exit

FTOS(config)#interface tenGigabitethernet 8/0
FTOS(conf-if-te-10/0)#no shutdown
FTOS(conf-if-te-10/0)#portmode hybrid
FTOS(conf-if-te-10/0)#switchport
FTOS(conf-if-te-10/0)#vlan-stack trunk
FTOS(conf-if-te-10/0)#exit

FTOS(config)#interface vlan 10
FTOS(conf-if-vlan)#vlan-stack compatible
FTOS(conf-if-vlan)#member Gi 7/0, Gi 3/10, TenGi 8/0
FTOS(conf-if-vlan)#exit

FTOS(config)#interface vlan 30
FTOS(conf-if-vlan)#untagged TenGi 8/0
FTOS(conf-if-vlan)#exit
FTOS(config)#

FTOS(config)#interface vlan 40
FTOS(conf-if-vlan)#tagged TenGi 8/0
FTOS(conf-if-vlan)#exit
FTOS(config)#
```

58

Virtual Link Trunking (VLT)

Virtual link trunking (VLT) is supported on the Dell Networking S5000 switch.

Virtual link trunking allows physical links between two chassis to appear as a single virtual link to the network core or other switches such as Edge, Access, or top-of-rack (ToR). VLT reduces the role of the spanning tree protocols by allowing link aggregation group (LAG) terminations on two separate distribution or core switches, and by supporting a loop-free topology. (You still need a spanning tree protocol to prevent the initial loop that may occur prior to VLT being established. After VLT is established, you may use the rapid spanning treee protocol (RSTP) to prevent loops from forming with new links that are incorrectly connected and outside the VLT domain.) VLT provides Layer 2 multipathing, creating redundancy through increased bandwidth, and enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

Prerequisites: Before you configure VLT, make sure that both VLT peer switches are running the same Dell Networking operating software (FTOS) version and are configured for RSTP as described in the "Virtual Link Trunking (VLT)" chapter in the *FTOS Configuration Guide*.

CAUTION: Dell Networking recommends not enabling Stacking and VLT simultaneously. If you enable both at the same time, unexpected behavior occurs.

back-up destination

Configure the IP address of the management interface on the remote VLT peer to be used as the endpoint of the VLT backup link for sending out-of-band hello messages.

S5000

Syntax

```
back-up destination ip-address [interval seconds]
```

Parameters

ip-address	Enter an IP address in dotted decimal format.
interval *seconds*	Enter the keyword `interval` to specify the time interval used to send hello messages. The range is 1 to 5 seconds.

Defaults	**1 second**
Command Modes	VLT DOMAIN

Command History

Version 9.0(1.3)	Introduced on the S5000.

clear vlt statistics

Clear the statistics on VLT operations.

S5000

Syntax `clear vlt statistics`

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands show vlt statistics – displays statistics on VLT operations.

delay-restore

Configure the delay in bringing up VLT ports after reload or peer-link restoration between the VLT peer switches.

S5000

Syntax `delay-restore`

Parameters

delay-restore	Enter the amount of time, in seconds, to delay bringing up the VLT ports after the VLTi device is reloaded or after the peer-link is restored between VLT peer switches. The range 1 to 1200. The default is **90 seconds**.

Defaults Not configured.

Command Modes VLT DOMAIN

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Use the `delay-restore` parameter to delay the system from bringing up the VLT port for a brief period to allow IGMP Snooping and Layer 3 routing protocols to converge. Use this feature:

- after a VLT device is reloaded.
- if the Peer VLT device was up at the time the VLTi link failed to the time when it was restored.

lacp ungroup member-independent

Enable BMP boot for the device connected to the LACP LAG or by a VLT peer device.

S5000

Syntax

`lacp ungroup member-independent {vlt | port-channel port-channel-id}`

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

LACP on the VLT ports (on a VLT switch or access device), which are members of the virtual link trunk, is not brought up until the VLT domain is recognized on the access device.

During boot-up in a stacking configuration, the system must be able to reach the DHCP server with the image and configuration image. During bootup, only untagged DHCP requests are sent to the DHCP server to receive an offer on static LAGs between switches. You must configure the DHCP server to start in Jumpstart mode. If the switches are connected using the LACP port-channel, similar to the VLT peer and ToR, use the `port-channel` parameter on the ToR side of the configuration to allow member ports of a completely un-grouped lacp port-channel to inherit vlan membership of that port channel to ensure untagged packets sent by a VLT peer device reach the DHCP server located on the ToR. To ungroup the vlt and port-channel configurations, use the `no lacp ungroup member-independent vlt` command on a VLT port channel, depending on whether the port channel is VLT or non-VLT.

peer-link port-channel

Configure the specified port channel as the chassis interconnect trunk between VLT peers in the domain.

S5000

Syntax

`peer-link port-channel port-channel-number {peer-down-vlan vlan id}`

Parameters

port-channel-number	Enter the port-channel number that acts as the interconnect trunk.
peer-down-vlan *vlan id*	(Optional) Configure the VLAN that the VLT peer link uses when the VLT peer is down.

Defaults

Not configured.

Command Modes

VLT DOMAIN

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Usage Information

Use the `peer-down-vlan` parameter to configure the VLAN from where the VLT peer forwards packets received over the VLTi from an adjacent VLT peer that is down. When a VLT peer with bare metal provisioning (BMP) is booting up, it sends untagged DHCP discover packets to its peer over the VLTi. Use this configuration to ensure that the DHCP discover packets are forwarded to the VLAN on the DHCP server.

primary-priority

Assign the priority for master election among VLT peers.

S5000

Syntax

```
[no] primary-priority
```

Parameters		
	value	To configure the primary role on a VLT peer, enter a lower value than the priority value of the remote peer. The range is 1 to 65535.

Default 32768

Command Modes VLT DOMAIN

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Usage Information

After you configure the VLT domain on each peer switch on both sides of the interconnect trunk, by default, the FTOS software elects a primary and secondary VLT peer device. Use the `priority` command to reconfigure the primary role of VLT peer switches.

show vlt

Displays status information about VLT domains currently configured on the switch.

S5000

Syntax

```
show vlt [brief | detail]
```

Default Not configured.

Command Modes EXEC

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The version shown in the `show vlt brief` output command displays the VLT version number which is different from the FTOS version number. VLT version numbers are begin with odd numbers such as 3 or 5.

Example (Brief)

```
FTOS(conf)#show vlt brief
VLT Domain Brief
------------------
Domain ID:                  10
Role:                       Primary
Role Priority:              32768
ICL Link Status:            Up
HeartBeat Status:           Not Established
VLT Peer Status:            Up
Version:                    5(1)
Local System MAC address:  00:01:e8:8b:14:3c
Remote System MAC address: 00:01:e8:8b:15:20
Remote system version:      5 (1)
```

Example (Detail)

```
FTOS# FTOS(conf-if-vl-100)#show vlt detail
Local LAG    Peer LAG    Local    Peer    Active VLANs
Id           Id          Status   Status
--------------------------------------------------------
10           10          UP     UP        100,200,300,400
```

show vlt backup-link

Displays information on the backup link operation.

S5000

Syntax `show vlt backup-link`

Default Not configured.

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS_VLTpeer1# show vlt backup-link

VLT Backup Link
-----------------
Destination:                 10.11.200.18
Peer HeartBeat status:       Up
HeartBeat Timer Interval:    1
HeartBeat Timeout:           3
UDP Port:                    34998
HeartBeat Messages Sent:     1026
HeartBeat Messages Received: 1025
```

show vlt counter

Displays the counter information.

S5000

Syntax `show vlt counter [arp| igmp-snoop | interface | mac]`

Parameters

arp	Enter the keyword `arp` to display the ARP counter information for the VLT.
igmp-snoop	Enter the keywords `igmp-snoop` to display the igmp-snooping counter information for the VLT
interface	Enter the keyword `interface` to display the interface counter information for the VLT.
mac	Enter the keyword `mac` to display the MAC address counter information for the VLT.

Default Not configured.

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If you do not add a parameter such as `arp` or `mac`, the output displays all of the counters.

Example

```
FTOS# show vlt counter
Total VLT counters
-------------------------
L2 Total MAC-Address Count :
IGMP MRouter Vlans count :
IGMP Mcast Groups count :
ARP entries count :
```

Example (igmp-snoop)

```
FTOS# show vlt counter igmp-snoop
Total IGMP VLT counters
----------------------
IGMP MRouter Vlans count : 1
IGMP Mcast Groups count  : 5
```

Example (port-channel)

```
FTOS#show vlt counter igmp-snoop interface port-channel 2
VLT Port-ID: 2 IGMP Counter
-----------------------
IGMP MRouter Vlans count : 0
IGMP Mcast Groups count  : 5

FTOS# show vlt counter igmp-snoop interface port-channel 100
VLT Port-ID: 100 IGMP Counter
-----------------------
IGMP MRouter Vlans count : 1
IGMP Mcast Groups count  : 0
Ve
```

show vlt role

Displays the VLT peer status, role of the local VLT switch, VLT system MAC address and system priority, and the MAC address and priority of the local VLT device.

S5000

Syntax `show vlt role`

Default Not configured.

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS_VLTpeer1# show vlt role

VLT Role
----------
VLT Role:                     Primary
System MAC address:           00:01:e8:8a:df:bc
System Role Priority:         32768
Local System MAC address:     00:01:e8:8a:df:bc
Local System Role Priority: 32768

FTOS_VLTpeer2# show vlt role

VLT Role
----------
VLT Role:                     Secondary
System MAC address:           00:01:e8:8a:df:bc
System Role Priority:         32768
Local System MAC address:     00:01:e8:8a:df:e6
Local System Role Priority: 32768
```

show vlt statistics

Displays statistics on VLT operations.

S5000

Syntax `show vlt statistics`

Default Not configured.

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

NOTE: The following Example shows the statistics for *all* of the VLT parameters. If you enter a specific keyword, such as `mac`, only the statistics for that VLT parameter displays.

Example

```
FTOS_VLTpeer1#show vlt statistics
VLT Statistics
----------------
HeartBeat Messages Sent:     930
HeartBeat Messages Received: 909
ICL Hello's Sent:            927
ICL Hello's Received:        910
Domain Mismatch Errors:      0
Version Mismatch Errors:     0
Config Mismatch Errors:      0

VLT MAC Statistics
----------------
L2 Info Pkts sent:6, L2 Mac-sync Pkts Sent:0
L2 Info Pkts Rcvd:3, L2 Mac-sync Pkts Rcvd:2
L2 Reg Request sent:1
L2 Reg Request rcvd:2
L2 Reg Response sent:1
L2 Reg Response rcvd:1

VLT Igmp-Snooping Statistics
-------------------------------
IGMP Info Pkts sent:     4
IGMP Info Pkts Rcvd:     1
IGMP Reg Request sent:   1
IGMP Reg Request rcvd:   2
IGMP Reg Response sent:  1
IGMP Reg Response rcvd:  1
IGMP PDU Tunnel Pkt sent: 5
IGMP PDU Tunnel Pkt rcvd: 10
IGMP Tunnel PDUs sent:    10
IGMP Tunnel PDUs rcvd:    19

VLT ARP Statistics
----------------
ARP Tunnel Pkts sent:0
ARP Tunnel Pkts Rcvd:0
ARP-sync Pkts Sent:0
ARP-sync Pkts Rcvd:0
ARP Reg Request sent:19
ARP Reg Request rcvd:10
```

Related Commands

clear vlt statistics – clears the statistics on VLT operations.

show vlt statistics igmp-snoop

Displays the informational packets and IGMP control PDUs that are exchanged between VLT peer nodes.

S5000

Syntax `show vlt statistics igmp-snoop`

Default Not configured.

Command Modes EXEC

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS_VLTpeer1#show vlt statistics igmp-snoop
VLT Igmp-Snooping Statistics
-------------------------------
IGMP Info Pkts sent:     4
IGMP Info Pkts Rcvd:     1
IGMP Reg Request sent:   1
IGMP Reg Request rcvd:   2
IGMP Reg Response sent:  1
IGMP Reg Response rcvd:  1
IGMP PDU Tunnel Pkt sent:5
IGMP PDU Tunnel Pkt rcvd:10
IGMP Tunnel PDUs sent:   10
IGMP Tunnel PDUs rcvd:   19
```

system-mac

Configure the MAC address for the VLT domain on a VLT peer switch.

S5000

Syntax `system-mac` *`mac-address`*

Parameters

mac-address	Enter a MAC address in the format aaaa.bbbb.cccc.

Default Automatically assigned based on the primary priority and MAC address of each VLT peer.

Command Modes VLT DOMAIN

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

When you create a VLT domain on a switch, FTOS automatically creates a VLT-system MAC address used for internal system operations. Use the `system-mac` command to explicitly define the MAC address for the domain. You must also reconfigure the same MAC address on the VLT peer switch.

Use this command to minimize the time required for the VLT system to synchronize the default MAC address of the VLT domain on both peer switches when one peer switch reboots.

unit-id

Explicitly configure the default unit ID of a VLT peer switch.

S5000

Syntax	`unit-id [0 | 1]`
Parameters	**0 | 1** — Configure the default unit ID of a VLT peer switch. Enter `0` for a unit with a lower MAC address or enter `1` for a unit with a higher MAC address.
Default	Automatically assigned based on the MAC address of each VLT peer. The peer with the lower MAC address is assigned unit 0; the peer with the higher MAC address is assigned unit 1.
Command Modes	VLT DOMAIN
Command History	**Version 9.0(1.3)** — Introduced on the S5000.
Usage Information	When you create a VLT domain on a switch, FTOS automatically assigns a unique unit ID (0 or 1) to each peer switch. The unit IDs are used for internal system operations. Use the `unit-id` command to explicitly configure the unit ID of a VLT peer. You must configure a different unit ID (0 or 1) on each peer switch. Use this command to minimize the time required for the VLT system to determine the unit ID assigned to each peer switch when one peer reboots.

vlt domain

Use this command to enable VLT on a switch, configure a VLT domain, enter VLT-domain configuration mode, set a VLT port delay time, set VLT priorities and configure a VLT peer link.

S5000

Syntax	`vlt domain` *`domain-id`*
Parameters	***domain-id*** — Enter the Domain ID number. You must configure the same domain ID on the peer switch. VLT uses the domain ID to automatically create a VLT MAC address for the domain. The range of domain IDs is 1 to 1000.
Command Modes	CONFIGURATION
Command History	**Version 9.0(1.3)** — Introduced on the S5000.

Usage Information	The VLT domain ID must be the same between the two VLT devices. If the domain ID is not the same, a syslog message is generated and VLT does not launch.
Related Commands	show vlt – uses the `show vlt brief` command to display the delay-restore value.

vlt-peer-lag port-channel

Associate the port channel to the corresponding port channel in the VLT peer for the VLT connection to an attached device.

S5000

Syntax

```
vlt-peer-lag port-channel id-number
```

Parameters

id-number	Enter the port-channel number that connects to another port channel in the VLT peer.

Defaults	Not configured.
Command Modes	INTERFACE PORT-CHANNEL

Command History

Version 9.0(1.3)	Introduced on the S5000.

59

Virtual Router Redundancy Protocol (VRRP)

The virtual router redundancy protocol (VRRP) is supported by the Dell Networking operating software (FTOS) on the S5000 switch.

This chapter has the following sections:

- IPv4 VRRP Commands
- IPv6 VRRP Commands

IPv4 VRRP Commands

The following are IPv4 VRRP commands.

advertise-interval

Set the time interval between VRRP advertisements.

S5000

Syntax `advertise-interval seconds`

To return to the default settings, use the `no advertise-interval` command.

Parameters

seconds	Enter a number of seconds. The range is 1 to 255. The default is **1 second**.

Defaults **1 second**

Command Modes INTERFACE-VRRP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information Dell Networking recommends keeping the default setting for this command. If you do change the time interval between VRRP advertisements on one router, you must change it on all routers.

authentication-type

Enable authentication of VRRP data exchanges.

S5000

Syntax

`authentication-type simple [`*`encryption-type`*`]` *`password`*

To delete an authentication type and password, use the `no authentication-type` command.

Parameters

simple	Enter the keyword `simple` to specify simple authentication.
encryption-type	(OPTIONAL) Enter one of the following numbers: • `0` (zero) for an un-encrypted (clear text) password. • `7` (seven) for hidden text password.
password	Enter a character string up to eight characters long as a password. If you do not enter an encryption-type, the password is stored as clear text.

Defaults

Not configured.

Command Modes

VRRP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The password is displayed in the `show config` output if the encryption-type is unencrypted or clear text. If you choose to encrypt the password, the `show config` output displays an encrypted text string.

clear counters vrrp

Clear the counters maintained on VRRP operations.

S5000

Syntax

`clear counters vrrp [`*`vrrp-id`*`]`

Parameters

vrrp-id	(OPTIONAL) Enter the number of the VRRP group ID. The range is 1 to 255.

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug vrrp

Allows you to enable debugging of VRRP.

S5000

Syntax

```
debug vrrp [vrrp-id] | [interface-type slot/port] | [interface]
| {all | packets | state | timer}
```

To disable debugging, use the `no debug vrrp [interface-type slot/port] | [interface][vrrp-id] {all | packets | state | timer}` command.

Parameters

interface-type slot/port	Enter the interface type followed by slot/port or number information to turn on debugging for specific interfaces. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
interface	Enter the `interface` keyword to enable debugging of all groups on all interfaces.
vrrp-id	(OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.
all	Enter the keyword `all` to enable debugging of all VRRP groups.
bfd	Enter the keyword `bfd` to enable debugging of all VFFP BFD interactions.
packets	Enter the keyword `packets` to enable debugging of VRRP control packets.
state	Enter the keyword `state` to enable debugging of VRRP state changes.
timer	Enter the keyword `timer` to enable debugging of the VRRP timer.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If no options are specified, debug is active on all interfaces and all VRRP groups.

description

Configure a short text string describing the VRRP group.

S5000

Syntax

`description text`

To delete a VRRP group description, use the `no description` command.

Parameters

text	Enter a text string up to 80 characters long.

Defaults

Not enabled.

Command Modes

VRRP

Command History

Version 9.0(1.3)	Introduced on the S5000.

disable

Disable a VRRP group.

S5000

Syntax

`disable`

To re-enable a disabled VRRP group, use the `no disable` command.

Defaults

Enabled.

Command Modes

VRRP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To enable VRRP traffic, assign an IP address to the VRRP group using the `virtual-address` command and enter `no disable`.

Related Commands

virtual-address – specifies the IP address of the virtual router.

hold-time

Specify a delay (in seconds) before a switch becomes the MASTER virtual router. By delaying the initialization of the VRRP MASTER, the new switch can stabilize its routing tables.

S5000

Syntax

`hold-time seconds`

To return to the default value, use the `no hold-time` command.

Parameters

seconds	Enter a number of seconds. The range is 0 to 65535. The default is **zero (0) seconds**.

Defaults **zero (0) seconds**

Command Modes VRRP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If a switch is a MASTER and you change the hold timer, you must disable and re-enable VRRP for the new hold timer value to take effect.

Related Commands disable – disables a VRRP group.

preempt

Permit a BACKUP router with a higher priority value to preempt or become the MASTER router.

S5000

Syntax

`preempt`

To prohibit preemption, use the `no preempt` command.

Defaults Enabled (that is, a BACKUP router can preempt the MASTER router).

Command Modes VRRP

Command History

Version 9.0(1.3)	Introduced on the S5000.

priority

Specify a VRRP priority value for the VRRP group. This value is used by the VRRP protocol during the MASTER election process.

S5000

Syntax `priority` *`priority`*

To return to the default value, use the `no priority` command.

Parameters

priority	Enter a number as the priority. Enter 255 only if the router's virtual address is the same as the interface's primary IP address (that is, the router is the OWNER). The range is 1 to 255. The default is **100**.

Defaults **100**

Command Modes VRRP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

To guarantee that a VRRP group becomes MASTER, configure the VRRP group's virtual address with same IP address as the interface's primary IP address and change the priority of the VRRP group to 255.

If you set the `priority` command to 255 and the `virtual-address` is not equal to the interface's primary IP address, an error message appears.

show config

View the non-default VRRP configuration.

S5000

Syntax `show config [verbose]`

Parameters

verbose	(OPTIONAL) Enter the keyword `verbose` to view all VRRP group configuration information, including defaults.

Command Modes VRRP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS(conf-if-vrid-4)#show con
 vrrp-group 4
  virtual-address 119.192.182.124
 !
```

show vrrp

View the VRRP groups that are active. If no VRRP groups are active, the FTOS returns `No Active VRRP group`.

S5000

Syntax

`show vrrp [vrrp-id] [interface-type slot/port] [brief] | [ipv6]`

Parameters

vrrp-id	(OPTIONAL) Enter the Virtual Router Identifier for the VRRP group to view only that group. The range is 1 to 255.
interface-type slot/port	(OPTIONAL) Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
brief	(OPTIONAL) Enter the keyword `brief` to view a table of information on the VRRP groups on the S5000.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output from the `show vrrp brief` command shown in the Example below.

Item	**Description**
Interface	Lists the interface type, slot and port on which the VRRP group is configured.
Grp	Displays the VRRP group ID.
Pri	Displays the priority value assigned to the interface. If the `track` command is configured to track that interface and the interface is disabled, the cost is subtracted from the priority value assigned to the interface.
Pre	States whether preempt is enabled on the interface.

- `Y` = Preempt is enabled.
- `N` = Preempt is not enabled.

State	Displays the operational state of the interface by using one of the following: • NA/IF (the interface is not available). • MASTER (the interface associated with the MASTER router). • BACKUP (the interface associated with the BACKUP router).
Master addr	Displays the IP address of the MASTER router.
Virtual addr(s)	Displays the virtual IP addresses of the VRRP routers associated with the interface.

Example (Brief)

```
FTOS>show vrrp brief
Interface Grp Pri Pre State Master addr     Virtual addr(s)
------------------------------------------------------------
Te        10/37   1   100 Y Master 200.200.200.200
200.200.200.201
Te        10/37   2   100 Y Master 200.200.200.200
200.200.200.202
    200.200.200.203
Te        10/37   3   100 Y Master 1.1.1.1          1.1.1.2
Te        10/37   4   100 Y Master 200.200.200.200
200.200.200.206

200.200.200.207
Te        10/37  254  254 Y Master 200.200.200.200
200.200.200.204

200.200.200.205
FTOS>
```

Usage Infromation

The following describes output from the `show vrrp` command shown in the Example below.

Line beginning with	Description
TenGigabitEthernet 12/3...	Displays the Interface, the VRRP group ID, and the network address. If the interface is not sending VRRP packets, 0.0.0.0 appears as the network address.
State: master...	Displays the interface's state: • Na/If (not available) • master (MASTER virtual router) • backup (BACKUP virtual router) the interface's priority and the IP address of the MASTER.
Hold Down:...	This line displays additional VRRP configuration information: • Hold Down displays the hold down timer interval in seconds. • Preempt displays TRUE if preempt is configured and FALSE if preempt is not configured.

	• AdvInt displays the Advertise Interval in seconds.
Adv rcvd:...	This line displays counters for the following: • Adv rcvd displays the number of VRRP advertisements received on the interface. • Adv sent displays the number of VRRP advertisements sent on the interface. • Gratuitous ARP sent displays the number of gratuitous ARPs sent.
Virtual MAC address	Displays the virtual MAC address of the VRRP group.
Virtual IP address	Displays the virtual IP address of the VRRP router to which the interface is connected.
Authentication:...	States whether authentication is configured for the VRRP group. If it is, the authentication type and the password are listed.
Tracking states..	This line is displayed if the `track` command is configured on an interface. Below this line, the following information on the tracked interface is displayed: • Dn or Up states whether the interface is down or up. • the interface type slot/port information.

Example

```
FTOS>show vrrp
------------------
TenGigabitEthernet 12/3, VRID: 1, Net: 10.1.1.253
State: Master, Priority: 105, Master: 10.1.1.253 (local)
Hold Down: 0 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Adv sent: 1862, Gratuitous ARP sent: 0
Virtual MAC address:
  00:00:5e:00:01:01
Virtual IP address:
  10.1.1.252
Authentication: (none)
Tracking states for 1 interfaces:
  Up TenGigabitEthernet 12/17 priority-cost 10
------------------
TenGigabitEthernet 12/4, VRID: 2, Net: 10.1.2.253
State: Master, Priority: 110, Master: 10.1.2.253 (local)
Hold Down: 10 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Adv sent: 1862, Gratuitous ARP sent: 0
Virtual MAC address:
  00:00:5e:00:01:02
Virtual IP address:
  10.1.2.252
Authentication: (none)
Tracking states for 2 interfaces:
  Up TenGigabitEthernet 2/1 priority-cost 10
  Up TenGigabitEthernet 12/17 priority-cost 10
FTOS>
```

track

Monitor an interface and lower the priority value of the VRRP group on that interface if it is disabled.

S5000

Syntax `track interface-type slot/port [priority-cost cost]`

To disable monitoring, use the `no track interface` command.

Parameters

interface-type slot/port	(OPTIONAL) Enter the interface type and slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
cost	(OPTIONAL) Enter a number as the amount to be subtracted from the priority value. The range is 1 to 254. The default is **10**.

Defaults cost = **10**

Command Modes VRRP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If the interface is disabled, the cost value is subtracted from the priority value and forces a new MASTER election if the priority value is lower than the priority value in the BACKUP virtual routers.

virtual-address

Configure up to 12 IP addresses of virtual routers in the VRRP group. You must set at least one virtual address for the VRRP group to start sending VRRP packets.

S5000

Syntax `virtual-address ip-address1 [... ip-address12]`

To delete one or more virtual IP addresses, use the `no virtual-address ip-address1 [... ip-address12]` command.

Parameters

ip-address1	Enter an IP address of the virtual router in dotted decimal format. The IP address must be on the same subnet as the interface's primary IP address.
... ip-address12	(OPTIONAL) Enter up to 11 additional IP addresses of virtual routers in dotted decimal format. Separate the IP addresses with a space. The IP addresses must be on the same subnet as the interface's primary IP address.

Defaults Not configured.

Command Modes VRRP

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The VRRP group only becomes active and sends VRRP packets when a virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

A system message appears after you enter or delete the `virtual-address` command.

To guarantee that a VRRP group becomes MASTER, configure the VRRP group's virtual address with the same IP address as the interface's primary IP address and change the priority of the VRRP group to 255.

You can ping the virtual addresses configured in all VRRP groups.

vrrp delay minimum

Set the delay time for VRRP initialization after an interface comes up.

S5000

Syntax `vrrp delay minimum seconds`

Parameters

seconds	Enter the number of seconds for the delay for VRRP initialization after an interface becomes operational. The range is 0 to 900 (0 indicates no delay).

Defaults 0

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command applies to a single interface. When used in conjunction with the `vrrp delay reload` CLI, the later timer rules the VRRP enabling. For example, if `vrrp delay reload` is 600 and the `vrrp delay minimum` is 300:

- When the system reloads, VRRP waits 600 seconds (10 minutes) to bring up VRRP on all interfaces that are up and configured for VRRP.
- When an interface comes up, whether as part of a system reload or an interface reload, the system waits 300 seconds (5 minutes) to bring up VRRP on that interface.

Related Command

vrrp delay reload – sets the delay time for VRRP initialization after a system reboot.

vrrp delay reload

Set the delay time for VRRP initialization after a system reboot.

S5000

Syntax

```
vrrp delay minimum seconds
```

Parameters

seconds	Enter the number of seconds for the delay. The range is 0 to 900 (0 indicates no delay).

Defaults

0

Command Modes

INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

This command applies to all the VRRP configured interfaces on a system. When used in conjunction with the `vrrp delay minimum` CLI, the later timer rules the VRRP enabling. For example, if `vrrp delay reload` is 600 and the `vrrp delay minimum` is 300:

- When the system reloads, VRRP waits 600 seconds (10 minutes) to bring up VRRP on all interfaces that are up and configured for VRRP.
- When an interface comes up, whether as part of a system reload or an interface reload, the system waits 300 seconds (5 minutes) to bring up VRRP on that interface.

You must save the configuration and reload the system for the delay timers to take affect.

Related Command

vrrp delay minimum – sets the delay time for VRRP initialization after a stack-unit reboot.

vrrp-group

Assign a VRRP ID to an interface. You can configure up to 12 VRRP groups per interface.

S5000

Syntax	`vrrp-group vrrp-id`
Parameters	*vrrp-id* — Enter a number as the group ID. The range is 1 to 255.
Defaults	Not configured.
Command Modes	INTERFACE
Command History	**Version 9.0(1.3)** — Introduced on the S5000.
Usage Information	The VRRP group only becomes active and sends VRRP packets when a virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.
Related Command	virtual-address – assigns up to 12 virtual IP addresses per VRRP group.

IPv6 VRRP Commands

The following are IPv6 VRRP commands.

The following commands apply to IPv4 and IPv6:

- advertise-interval
- description
- disable
- hold-time
- preempt
- priority
- show config
- track
- virtual-address

clear counters vrrp ipv6

Clear the counters recorded for IPv6 VRRP groups.

S5000

Syntax

```
clear counters vrrp ipv6 [vrid ]
```

Parameters

vrid	(OPTIONAL) Enter the number of an IPv6 VRRP group. The range is 1 to 255.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

debug vrrp ipv6

Allows you to enable debugging of VRRP.

S5000

Syntax

```
debug vrrp ipv6 interface-type slot/port | [interface] | [vrid]
{all | packets | state | timer}
```

Parameters

interface-type slot/port	Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
interface	Enter the `interface` keyword to enable debugging of all groups on all interfaces.
vrid	(OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.
all	Enter the keyword `all` to enable debugging of all VRRP groups.
bfd	Enter the keyword `bfd` to enable debugging of all VFFP BFD interactions.

database	Enter the keyword `database` to display changes related to group, prefix, and interface entries in the VRRP table.
packets	Enter the keyword `packets` to enable debugging of VRRP control packets.
state	Enter the keyword `state` to enable debugging of VRRP state changes
timer	Enter the keyword `timer` to enable debugging of the VRRP timer.

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information If no options are specified, debug is active on all interfaces and all VRRP groups.

show vrrp ipv6

View the IPv6 VRRP groups that are active. If no VRRP groups are active, the FTOS returns `No Active VRRP group`.

S5000

Syntax `show vrrp ipv6 [vrid] [interface-type slot/port] [brief]`

Parameters

vrid	(OPTIONAL) Enter the virtual router identifier for the VRRP group to view only that group. The range is 1 to 255.
interface-type slot/port	Enter the interface type followed by slot/port or number information. Valid slot numbers are 0-11. The valid port numbers for each interface type are listed below. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by slot/port numbers. The port range is 0 to 63. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by slot/port numbers. The ports are 48, 52, 56, and 60. • For a Port Channel interface, enter the keywords `port-channel` followed by a number from 1 to 128. • For a VLAN interface, enter the keyword `vlan` followed by a VLAN id number from 1 to 4094.
brief	(OPTIONAL) Enter the keyword `brief` to view a table of information on the VRRP groups on the S5000.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The following describes output from the `show vrrp ipv6` command shown in the Example below.

Line beginning with	Description
TenGigabitEthernet...	Displays the Interface, the VRRP group ID, and the network address. If the interface is no sending VRRP packets, 0.0.0.0 appears as the network address.
VRF	VRF instance to which the interface (on which the VRRP group is configured) belongs.
State: master...	Displays the interface's state: • Na/If (not available). • master (MASTER virtual router). • backup (BACKUP virtual router). the interface's priority and the IP address of the MASTER.
Hold Down:...	This line displays additional VRRP configuration information: • Hold Down displays the hold down timer interval in seconds. • Preempt displays TRUE if preempt is configured and FALSE if preempt is not configured. • AdvInt displays the Advertise Interval in seconds.
Adv rcvd:...	This line displays counters for the following: • Adv rcvd displays the number of VRRP advertisements received on the interface. • Adv sent displays the number of VRRP advertisements sent on the interface. • Bad pkts rcvd displays the number of invalid packets received on the interface.
Virtual MAC address	Displays the virtual MAC address of the VRRP group.
Virtual IP address	Displays the virtual IP address of the VRRP router to which the interface is connected.
Tracking states...	Displays information on the tracked interfaces or objects configured for a VRRP group (`track` command), including: • UP or DOWN state of the tracked interface or object (Up or Dn).

- Interface type and slot/port or object number, description, and time since the last change in the state of the tracked object.
- Cost to be subtracted from the VRRP group priority if the state of the tracked interface/object goes DOWN.

Example

```
FTOS#show vrrp ipv6
------------------
TenGigabitEthernet 5/6, IPv6 VRID: 255, Version: 3, Net:
fe80::201:e8ff:fe7a:6bb9
VRF: 0 default-vrf
State: Master, Priority: 101, Master: fe80::201:e8ff:fe7a:6bb9
(local)
Hold Down: 0 centisec, Preempt: TRUE, AdvInt: 100 centisec
Accept Mode: FALSE, Master AdvInt: 100 centisec
Adv rcvd: 0, Bad pkts rcvd: 0, Adv sent: 64
Virtual MAC address:
  00:00:5e:00:02:ff
Virtual IP address:
  1::255 fe80::255
```

vrrp-ipv6-group

Assign an interface to a VRRP group.

S5000

Syntax `vrrp-ipv6-group` *`vrid`*

Parameters

vrid	Enter the virtual-router ID number of the VRRP group. The VRID range is 1 to 255.

Defaults Not configured.

Command Modes INTERFACE

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information The VRRP group only becomes active and sends VRRP packets when a link-local virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

Related Commands virtual-address – assigns up to 12 virtual IP addresses per VRRP group.

60

Debugging and Diagnostics

The basic debugging and diagnostic commands are supported by the Dell Networking operating software (FTOS) on the S5000 switch.

This chapter contains the following sections:

- Offline Diagnostic Commands
- Buffer Tuning Commands
- Hardware Commands

Offline Diagnostic Commands

The offline diagnostics test suite is useful for isolating faults and debugging hardware. While tests are running, FTOS results are saved as a text file (TestReport-SU-X.txt) in the flash directory. This `show file` command is available only on master and standby.

Important Points to Remember

- Offline diagnostics can only be run when the unit is offline.
- You can only run offline diagnostics on a unit to which you are connected via the console. In other words, you cannot run diagnostics on a unit to which you are connected to via a stacking link.
- Diagnostic results are printed to the screen. FTOS does not write them to memory.
- Diagnostics only test connectivity, not the entire data path.

diag stack-unit

Run offline diagnostics on a stack unit.

S5000

Syntax

```
diag stack-unit unit-number [alllevels | level0 | level1 |
level2] verbose testname
```

Parameters

unit-number	Enter the keywords `stack-unit` followed by the stack-unit number. The range is 0 to 11.
alllevels	Enter the keyword `alllevels` to run the complete set of offline diagnostic tests.
level0	Enter the keyword `level0` to run Level 0 diagnostics. Level 0 diagnostics check for the presence of various components and

	perform essential path verifications. In addition, they verify the identification registers of the components on the board.
level1	Enter the keyword `Level1` to run Level 1 diagnostics. Level 1 diagnostics is a smaller set of diagnostic tests with support for automatic partitioning. They perform status/self test for all the components on the board and test their registers for appropriate values. In addition, they perform extensive tests on memory devices (for example, SDRAM, flash, NVRAM, EEPROM, and CPLD) wherever possible. There are no tests on 10G links. At this level, stack ports are shut down automatically.
level2	Enter the keyword `level2` to run Level 2 diagnostics. Level 2 diagnostics are a full set of diagnostic tests with no support for automatic partitioning. Level 2 diagnostics are used primarily for on-board loopback tests and more extensive component diagnostics. Various components on the board are put into Loopback mode and test packets are transmitted through those components. These diagnostics also perform snake tests using VLAN configurations. You must physically remove the unit from the stack to test 10G links.
verbose	Enter the keyword `verbose` to run the diagnostic in Verbose mode. Verbose mode gives more information in the output than Standard mode.
testname	Enter the keyword `level2` to run a specific test case. Enclose the test case name in double quotes (“ ”). For example: `diag stack-unit 1 level1 testname “first”`.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

offline stack-unit

Place a stack unit in the offline state.

S5000

Syntax `offline stack-unit` *`unit-number`*

Parameters

stack-unit ***unit-number***	Enter the keywords `stack-unit` followed by the unit number. The range is 0 to 11.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You cannot enter this command on a Master or Standby unit.

The system reboots when the off-line diagnostics complete. This is an automatic process. A warning message appears when the `offline stack-unit` command is implemented.

```
Warning - Diagnostic execution will cause stack-unit to reboot
after completion of diags.
Proceed with Offline-Diags [confirm yes/no]:y
```

Related Commands

show environment – views the S5000 component status (for example, temperature, voltage).

online stack-unit

Place a stack unit in the online state.

S5000

Syntax

`online stack-unit unit-number`

Parameters

stack-unit *unit-number*	Enter the keywords `stack-unit` followed by the unit number. The range is 0 to 11.

Defaults

none

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

You cannot enter this command on a Master or Standby unit.

The system reboots when the off-line diagnostics complete. This is an automatic process. A warning message appears when the `offline stack-unit` command is implemented.

```
Warning - Diagnostic execution will cause stack-unit to reboot
after completion of diags.
Proceed with Offline-Diags [confirm yes/no]:y
```

Related Commands

show environment – views the S5000 system component status (for example, temperature, voltage).

Buffer Tuning Commands

The following sections detail the buffer tuning commands.

WARNING: Altering the buffer allocations is a sensitive operation. Do not use any buffer tuning commands without first contacting the Dell Networking Technical Assistance Center (TAC).

buffer-profile (Configuration)

Create a buffer profile that can be applied to an interface.

S5000

Syntax

```
buffer-profile global {1Q|4Q}
```

Parameters

global	Apply one of two pre-defined buffer profiles to all of the port-pipes in the system.
1Q	Enter the keyword `1Q` to choose a pre-defined buffer profile for single queue (for example, non-QoS) applications.
4Q	Enter the keyword `4Q` to choose a pre-defined buff fer profile for four queue (for example, QoS) applications.

Defaults **global 4Q**

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information

The `buffer-profile global` command fails if you have already applied a custom buffer-profile on an interface. Similarly, when you configure `buffer-profile global`, you cannot apply buffer-profile on any interface.

If the default buffer-profile (4Q) is active, FTOS displays an error message instructing you to remove the default configuration using the `no buffer-profile global` command.

You must reload the system for the global buffer-profile to take effect.

Related Commands

buffer (Buffer Profile) – allocates an amount of dedicated buffer space, dynamic buffer space, or packet pointers to queues 0 to 3.

show buffer-profile stack-unit

Display the buffer profile that is applied to a stack-unit.

S5000

Syntax `show buffer-profile stack—unit unit-number`

Parameters

stack-unit *unit-number*	Enter the keyword `stack-unit` followed by the unit number. The range is 0 to 11. If you do not type a unit number, FTOS displays buffer-profiles for all units.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (single unit)

```
FTOS#show buffer-profile stack-unit 0
Stack-Unit  Current Buffer-Profile   Next-Boot Buffer-Profile
----------  ----------------------   ------------------------
0           Default (Dynamic)        Default (Dynamic)

FTOS#
```

Related Commands buffer-profile (Configuration) – creates a buffer profile that can be applied to an interface.

Hardware Commands

These commands display information from a hardware sub-component or ASIC.

clear hardware stack-unit

Clear statistics from selected hardware components.

S5000

Syntax

```
clear hardware stack-unit unit-number {counters | unit port-
pipe counters | cpu data-plane statistics | cpu party-bus
statistics | stack-port stacking-port-number}
```

Parameters

stack-unit *unit-number*	Enter the keyword `stack-unit` followed by the unit number. The range is 0 to 11. Then enter one of the following command options to clear a specific collection of data.

counters	Enter the keyword `counters` to clear the counters on the selected stack member.
unit ***port-pipe*** **counters**	Enter the keyword `unit` along with a port-pipe number, from 0 to 1, followed by the keyword counters to clear the counters on the selected port-pipe. **NOTE:** S25 models (S25N, S25P, S25V, etc.) have only port-pipe 0.
cpu data-plane statistics	Enter the keywords `cpu data-plane statistics` to clear the data plane statistics.
cpu party-bus statistics	Enter the keywords `cpu party-bus statistics` to clear the management statistics.
stack-port ***stacking-port-number***	Enter the keywords `stack-port` followed by the port number of the stacking port to clear the statistics of the particular stacking port. The range is 0 to 52.

Defaults none

Command Modes EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Related Commands show hardware stack-unit – displays the data plane or management plane input and output statistics of the designated component of the designated stack member.

clear hardware system-flow

Clear system-flow statistics from selected hardware components.

S5000

Syntax `clear hardware system-flow layer2 stack-unit` *`unit-number`* `port-set` *`port-pipe`* `counters`

Parameters

stack-unit ***unit-number***	Enter the keywords `stack-unit` followed by 0 to 11 for the stack unit number and then enter one of the following command options to clear a specific collection of data.
port-set ***port-pipe*** **counters**	Enter the keyword `port-set` followed by a port-pipe number. Valid ports are 0 or 1. Then enter the keyword `counters` to clear the system-flow counters on the selected port-pipe. **NOTE:** S25 models (S25N, S25P, S25V, etc.) have only port-pipe 0.

Defaults none

Command Modes	EXEC Privilege
Command History	**Version 9.0(1.3)** Introduced on the S5000.
Related Commands	show hardware stack-unit – displays the data plane or management plane input and output statistics of the designated component of the designated stack member.

hardware watchdog

Set the watchdog timer to trigger a reboot and restart the system.

S5000

Syntax `hardware watchdog`

Defaults Enabled.

Command Modes CONFIGURATION

Command History

Version 9.0(1.3)	Introduced on the S5000.

Usage Information This command enables a hardware watchdog mechanism that automatically reboots an FTOS switch/ router with a single unresponsive unit. This is a last resort mechanism intended to prevent a manual power cycle.

show hardware layer2 acl

Display Layer 2 ACL data for the selected stack member and stack member port-pipe.

S5000

Syntax `show hardware layer2 acl stack-unit` *`unit-number`* `port-set` *`port-pipe`*

Parameters

stack-unit ***unit-number***	Enter the keyword `stack-unit` followed by the unit number. The range is 0 to 11.
port-set ***port-pipe***	Enter the keyword `port-set` followed by a port-pipe number. Valid ports are 0 or 1.

Defaults none

Command Modes EXEC Privilege

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

show hardware layer3

Display Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

S5000

Syntax

```
show hardware layer3 {acl | qos} stack-unit unit-number port-
set port-pipe
```

Parameters

acl | qos	Enter either the keyword `acl` or the keyword `qos` to select between ACL or QoS data.
stack-unit *unit-number*	Enter the keyword `stack-unit` followed by the unit number. The range is 0 to 11.
port-set *port-pipe*	Enter the keyword `port-set` followed by a port-pipe number. Valid ports are 0 or 1.

Defaults none

Command Modes EXEC Privilege

Command History		
	Version 9.0(1.3)	Introduced on the S5000.

show hardware stack-unit

Display the data plane or management plane input and output statistics of the designated component of the designated stack member.

S5000

Syntax

```
show hardware stack-unit unit-number {buffer [buffer unit |
port [(0-27) | all] total buffer | buffer unit (1) port (0-64)
queue [(0-14) | all] buffer-info]} {cpu data-plane statistics
[stack-port 0-52] | cpu party-bus statistics | drops [unit 0-1
[port 0-27]] | stack-port 0-52 | unit 0-1 {counters | details |
port-stats [detail] | register}}
```

Parameters

stack-unit *unit-number* {*command-option*}	Enter the keywords `stack-unit` followed by the unit number. The range is 0 to 11. Then enter one of the following command options to display a collection of data based on the option entered.
buffer	Enter the keyword `buffer`, optionally followed by the keywords `total-buffer` to show the total buffer statistics per stack-unit. Enter the keywords `buffer unit` then `total-buffer` to display the buffer details per unit and mode of allocation. To display the forwarding plane statistics containing the packet buffer usage per port per stack-unit, enter the keywords `buffer unit` followed by port and the port number (*0-64* or `all`), then `buffer-info`. To display the forwarding plane statistics containing the packet buffer statistics per COS per port, enter the keywords `buffer unit` and `port` (*0-64*), and `queue` (*0-14* or `all`), and `buffer-info`. The buffer unit default is **1**.
cpu data-plane statistics	Enter the keywords `cpu data-plane statistics`, optionally followed by the keywords `stack port` and its number, 0 to 52, to display the data plane statistics, which shows the High Gig (`Higig`) port raw input/output counter statistics to which the stacking module is connected.
cpu party-bus statistics	Enter the keywords `cpu party-bus statistics`, to display the Management plane input/output counter statistics of the pseudo party bus interface.
drops [unit *0-1* [port *0-27*]]	Enter the keyword `drops` to display internal drops on the selected stack member. Optionally, use the keyword `unit` with `0` or `1` to select port-pipe 0 or 1, and then use `port` *0-27* to select a port on that port-pipe.
stack-port 0-52	Enter the keywords `stack-port` and a stacking port number to select a stacking port for which to display statistics. Identify the stack port number as you would to identify a 10G port that was in the same place in one of the rear modules.
unit *0-1* {counters | details | port-stats [detail] | register}	Enter the keyword `unit` followed by `0` or `1` for port-pipe 0 or 1, and then enter one of the following keywords to troubleshoot errors on the selected port-pipe and to give status on why a port is not coming up to register level: `counters`, `details`, `port-stats [detail]`, or `register`.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example (Data-Plane)

```
FTOS#show hardware stack-unit 0 cpu data-plane statistics

bc pci driver statistics for device:
 rxHandle        :1499
 noMhdr          :0
 noMbuf          :0
 noClus          :0
 recvd           :1499
 dropped         :0
 recvToNet       :1499
 rxError         :0
 rxFwdError      :0
 rxDatapathErr   :0
 rxPkt(COS0)     :0
 rxPkt(COS1)     :0
 rxPkt(COS2)     :0
 rxPkt(COS3)     :0
 rxPkt(COS4)     :0
 rxPkt(COS5)     :0
 rxPkt(COS6)     :0
 rxPkt(COS7)     :1499
 rxPkt(UNIT0)    :1499
 transmitted     :1979
 txRequested     :1979
 noTxDesc        :0
 txError         :0
 txReqTooLarge   :0
 txInternalError :0
 txDatapathErr   :0
 txPkt(COS0)     :0
 txPkt(COS1)     :0
 txPkt(COS2)     :0
 txPkt(COS3)     :0
 txPkt(COS4)     :0
 txPkt(COS5)     :0
 txPkt(COS6)     :0
 txPkt(COS7)     :0
 txPkt(UNIT0)    :0

FTOS#
```

Example (Party-Bus)

```
FTOS#show hardware stack-unit 0 cpu party-bus statistics
Input Statistics:
    0 packets, 0 bytes
    0 dropped, 0 errors
Output Statistics:
    0 packets, 0 bytes
    0 errors
FTOS#
```

Example (Drops)

```
FTOS#sh hard stack-unit 0 drops
UNIT No: 0
Total Ingress Drops: 0
Total IngMacDrops:   0
Total MmuDrops:      0
Total EgMacDrops:    0
Total Egress Drops:  0
FTOS#
```

Example (Drops Unit)

```
FTOS#show hard stack-unit 0 drops unit 0

User   Port    Ingress IngMac  Total Mmu EgMac  Egress
Port   Number  Drops   Drops   Drops     Drops  Drops
 0     1       0       0       0         0      0
 1     2       0       0       0         0      0
 2     3       0       0       0         0      0
 3     4       0       0       0         0      0
!--------------- output truncated --------------!
```

Example (Port-Stats)

```
FTOS#show hardware stack-unit 0 unit 0 port-stats
ena/ speed/ link auto  STP   lrn  inter   max  loop
port link duplex  scan neg? state pause discrd ops face frame
back
xe0  up   10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe1  !ena 10G FD   SW  No   Forward     RX   None    F  XGMII
1550
xe2  !ena 10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe3  !ena 10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe4  !ena 10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe5  !ena 10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe6  up   10G FD   SW  No   Forward     RX  Untag   FA  XGMII
2496
xe7  up   10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe8  !ena 10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe9  !ena 10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe10 down 10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe11 up   10G FD   SW  No   Forward     RX  Untag   FA  XGMII
2496
xe12 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe13 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe14 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe15 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe16 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe17 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe18 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe19 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe20 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe21 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe22 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe23 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
```

```
xe24 !ena 10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe25 !ena 10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe26 up   10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe27 up   10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe28 up   10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe29 up   10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe30 !ena 10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe31 !ena 10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe32 !ena 10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe33 !ena 10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe34 !ena 10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe35 !ena 10G FD   SW  No   Forward     RX    Tag    F  XGMII
1550
xe36 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe37 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe38 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe39 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe40 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe41 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe42 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe43 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe44 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe45 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe46 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe47 !ena  1G FD   SW  Yes  Forward          None   FA   GMII
16356
xe48 !ena 40G FD   SW  No   Forward           Tag    F  XLAUI
1550
xe49 !ena 40G FD   SW  No   Forward           Tag    F  XLAUI
1550
xe50 !ena 40G FD   SW  No   Forward           Tag    F  XLAUI
1550
xe51 !ena 40G FD   SW  No   Forward           Tag    F  XLAUI
1550
!-------------------- output truncated ---------------------!
FTOS#
```

Example (Total-Buffer)

```
FTOS#show hardware stack-unit 0 buffer unit 0 total-buffer
-----  Buffer Details for Unit 0 -----
 Used Packet Buffer for the Unit: 46080
 Is Dynamic Packet Buffer allocate for the unit: TRUE
```

```
FTOS#
```

Example (Buffer-Info)

```
FTOS#show hardware stack-unit 0 buffer unit 0 port 1 buffer-
info
-----  Buffer Stats for Unit 0 Port 1 -----
 Maximum Shared Limit for the Port: 38336
 Default Packet Buffer allocate for the Port: 120
 Used Packet Buffer for the Port: 0

FTOS#
```

Related Commands

clear hardware system-flow – clears the statistics from selected hardware components.

show interfaces stack-unit – displays information on all interfaces on a specific S5000 stack member.

show processes cpu – displays the CPU usage information based on the processes running in an S5000.

show system – displays the current status of all the stack members or a specific member.

show hardware system-flow

Display Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

S5000

Syntax

```
show hardware system-flow layer2 stack-unit unit-number port-
set port-pipe [counters]
```

Parameters

acl | qos	For the selected stack member and stack member port-pipe, display which system flow entry the packet hits and what queue the packet takes as it dumps the raw system flow tables.
stack-unit *unit-number*	Enter the keyword `stack-unit` followed by the unit number. The range is 0 to 11.
port-set *port-pipe* [counters]	Enter the keyword `port-set` followed by a port-pipe number. Valid ports are 0 or 1. (OPTIONAL) Enter the keyword `counters` to display hit counters for the selected ACL or QoS option.

Defaults

none

Command Modes

EXEC Privilege

Command History

Version 9.0(1.3)	Introduced on the S5000.

Example

```
FTOS#show hardware system-flow layer2 stack-unit 0 port-set 0
counters
-----------------------------------------------------------
```

```
EntryId Description                  #HITS
-----------------------------------------------------------
2048    STP BPDU Redirects            0
2047    LLDP BPDU Redirects           0
2045    LACP traffic Redirects        0
2044    GVRP traffic Redirects        0
2043    ARP Reply Redirects           0
2042    802.1x frames Redirects       0
2041    VRRP frames Redirects         0
2040    GRAT ARP                      0
2039    DROP Cases                    0
2038    OSPF1 STUB                    0
2037    OSPF2 STUB                    0
2036    VRRP STUB                     0
2035    L2_DST_HIT+BC MAC+VLAN 4095   0
2034    L2_DST_HIT+BC MAC             0
2033    Catch all                     0
384     OSPF[224.0.0.5] Packets       0
383     OSPF[224.0.0.6] Packets       0
382     VRRP Packets                  0
380     BCast L2_DST_HIT on VLAN 4095 0
379     BCAST L2_DST_HIT Packets      0
4       Unknown L2MC Packets          0
3       L2DLF Packets                 0
2       L2UCAST Packets               0
1       L2BCASTPackets                0
25
FTOS#
```

Example

```
param1=0(0x00)},
   action={act=CosQCpuNew, param0=7(0x07), param1=0(0x00)},
   action={act=CopyToCpu, param0=0(0x00), param1=0(0x00)},
   action={act=UpdateCounter, param0=1(0x01), param1=0(0x00)},
   meter=NULL,
   counter={idx=1, mode=0x01, entries=1}

############## FP Entry for redirecting LACP traffic to CPU
Port ############
   EID 2045: gid=1,
   slice=15, slice_idx=0x02, prio=0x7fd, flags=0x82, Installed
   tcam: color_indep=0, higig=0, higig_mask=0,
   KEY=0x00000000 00000000 00000000 0180c200 00020000 00000000
00000000
, FPF4=0x00
   MASK=0x00000000 00000000 00000000 ffffffff ffff0000
00000000 00000000
,       0x00
    action={act=Drop, param0=0(0x00), param1=0(0x00)},
    action={act=CosQCpuNew, param0=7(0x07), param1=0(0x00)},
    action={act=CopyToCpu, param0=0(0x00), param1=0(0x00)},
    action={act=UpdateCounter, param0=1(0x01), param1=0(0x00)},
    meter=NULL,
    counter={idx=2, mode=0x01, entries=1}

################# FP Entry for redirecting GVRP traffic to RSM
###########
    EID 2044: gid=1,
    slice=15, slice_idx=0x03, prio=0x7fc, flags=0x82, Installed
    tcam: color_indep=0, higig=0, higig_mask=0,
KEY=0x00000000 00000000 00000000 0180c200 00210000 00000000
00000000
, FPF4=0x00
MASK=0x00000000 00000000 00000000 ffffffff ffff0000 00000000
```

```
00000000
,    0x00
    action={act=Drop, param0=0(0x00), param1=0(0x00)},
    action={act=CosQCpuNew, param0=7(0x07), param1=0(0x00)},
    action={act=CopyToCpu, param0=0(0x00), param1=0(0x00)},
    action={act=UpdateCounter, param0=1(0x01), param1=0(0x00)},
    meter=NULL,
    counter={idx=3, mode=0x01, entries=1}

################# FP Entry for redirecting ARP Replies to RSM
#############
    EID 2043: gid=1,
    slice=15, slice_idx=0x04, prio=0x7fb, flags=0x82, Installed
    tcam: color_indep=0, higig=0, higig_mask=0,
KEY=0x00000000 00000000 00000000 00000000 00000000 00000806
00001600
, FPF4=0x00
MASK=0x00000000 00000000 00000000 00000000 00000000 0000ffff
00001600
,    0x00
    action={act=Drop, param0=0(0x00), param1=0(0x00)},
    action={act=CosQCpuNew, param0=6(0x06), param1=0(0x00)},
    action={act=CopyToCpu, param0=0(0x00), param1=0(0x00)},
    action={act=UpdateCounter, param0=1(0x01), param1=0(0x00)},
!--------- output truncated -----------------!
```

61

ICMP Message Types

This chapter lists and describes the possible ICMP message type resulting from a ping. The first three columns list the possible symbol or type/code. For example, you would receive a ! or 03 as an echo reply from your ping.

ICMP Messages and Their Definitions.

Symbol	Type	Code	Description	Query	Error
.			Timeout (no reply)		
!	0	3	echo reply	.	
U	3		destination unreachable:		
		0	network unreachable		.
		1	host unreachable		.
		2	protocol unreachable		.
		3	port unreachable		.
		4	fragmentation needed but don’t fragment bit set		.
		5	source route failed		.
		6	destination network unknown		.
		7	destination host unknown		.
		8	source host isolated (obsolete)		.
		9	destination network administratively prohibited		.
		10	destination host administratively prohibited		.
		11	network unreachable for TOS		.
		12	host unreachable for TOS		.
		13	communication administratively prohibited by filtering		.
		14	host precedence violation		.
		15	precedence cutoff in effect		.
C	4	0	source quench		.
	5		redirect		.
		0	redirect for network		.

Symbol	Type	Code	Description	Query	Error
		1	redirect for host		.
		2	redirect for type-of-service and network		.
		3	redirect for type-of-service and host		.
	8	0	echo request	.	
	9	0	router advertisement	.	
	10	0	router solicitation	.	
&	11		time exceeded:		
		0	time-to-live equals 0 during transit		.
		1	time-to-live equals 0 during reassembly		.
	12		parameter problem:		
		1	IP header bad (catchall error)		.
		2	required option missing		.
	13	0	timestamp request	.	
	14	0	timestamp reply	.	
	15	0	information request (obsolete)	.	
	16	0	information reply (obsolete)	.	
	17	0	address mask request	.	
	18	0	address mask reply	.	

62

SNMP Traps

This chapter lists the traps sent by the Dell Networking operating software (FTOS). Each trap is listed by the fields Message ID, Trap Type, and Trap Option.

Message ID	Trap Type	Trap Option
COLD_START	SNMP	COLDSTART
`%SNMP-5-SNMP_COLD_START: SNMP COLD_START trap sent.`		
WARM_START	SNMP	WARMSTART
COPY_CONFIG_COMPLETE	SNMP	NONE
`SNMP Copy Config Command Completed`		
LINK_DOWN	SNMP	LINKDOWN
`%IFA-1-PORT_LINKDN: changed interface state to down:%d`		
LINK_UP	SNMP	LINKUP
`%IFA-1-PORT_LINKUP: changed interface state to up: %d`		
AUTHENTICATION_FAIL	SNMP	AUTH
`%SNMP-3-SNMP_AUTH_FAIL: SNMP Authentication failed.Request with invalid community string.`		
EGP_NEIGHBOR_LOSS	SNMP	NONE
OSTATE_DOWN	SNMP	LINKDOWN
`%IFM-1-OSTATE_DN: changed interface state to down: %s` `%IFM-5-CSTATE_DN:Changed interface Physical state to down: %s`		
OSTATE_UP	SNMP	LINKUP
`%IFM-1-OSTATE_UP: changed interface state to up:%s` `%IFM-5-CSTATE_UP: Changed interface Physical state to up: %s`		
RMON_RISING_THRESHOLD	SNMP	NONE
`%STKUNIT1-M:CP %SNMP-4-RMON_RISING_THRESHOLD: RMON rising threshold alarm from SNMP OID <oid>`		
RMON_FALLING_THRESHOLD	SNMP	NONE
`%STKUNIT1-M:CP %SNMP-4-RMON_FALLING_THRESHOLD: RMON falling threshold alarm from SNMP OID <oid>`		
RMON_HC_RISING_THRESHOLD	SNMP	NONE

Message ID	Trap Type	Trap Option
`%STKUNIT1-M:CP %SNMP-4-RMON_HC_RISING_THRESHOLD: RMON high-capacity rising threshold alarm from SNMP OID <oid>`		
RMON_HC_FALLING_THRESHOLD	SNMP	NONE
`%STKUNIT0-M:CP %SNMP-4-RMON_HC_FALLING_THRESHOLD: RMON high-capacity falling threshold alarm from SNMP OID <oid>`		
RESV	NONE	NONE
N/A		
CHM_STACK-UNIT_UP	ENVMON	NONE
`%RAM-5-STACK_STATE: Stack unit 0 is in Active State` `%RAM-5-STACK_STATE: Stack unit 1 is in Standby State`		
CHM_STACK-UNIT_DOWN	ENVMON	NONE
`%CHMGR-2-STACK_UNIT_DOWN: Stack unit 0 down - hard reset` %CHMGR-2-STACK_UNIT_DOWN: Stack unit 0 down - card removed		
CHM_STACK_UNIT_PRIMARY	ENVMON	NONE

`%RAM-5-COLD_FAILOVER: Stack unit 0 Failover Completed`
`%RAM-5-HOT_FAILOVER: Stack unit 0 Failover Completed`
`%RAM-5-FAST_FAILOVER: Stack unit 0 Failover Completed`		

PS_UP	ENVMON	SUPPLY
`%STKUNIT4-M:CP %CHMGR-0-PS_UP: Power supply 1 in unit 4 is up`		
MINOR_TEMP	ENVMON	TEMP
`%STKUNIT4-M:CP %CHMGR-2-MINOR_TEMP: Minor alarm: Unit 4 BASE BOARD (Sensor0 temperature reaches minor threshold of 95-100 C)`		
MINOR_TEMP_CLR	ENVMON	TEMP
`%STKUNIT4-M:CP %CHMGR-5-MINOR_TEMP_CLR: Minor alarm cleared: Unit 4 BASE BOARD (Sensor0 temperature is within threshold of 95-100 C)`		
MAJOR_TEMP	ENVMON	TEMP
`%STKUNIT4-M:CP %CHMGR-2-MAJOR_TEMP: Major alarm: Unit 4 Module 1 (Sensor0 temperature reaches major threshold of 76-76 C)`		
MAJOR_TEMP_CLR	ENVMON	TEMP
`%STKUNIT4-M:CP %CHMGR-2-MAJOR_TEMP_CLR: Major alarm cleared: Unit 4 Module 1 (Sensor0 temperature is within threshold of 76-76 C)`		
PSU_FAN_STATUS	ENVMON	FAN

Message ID	Trap Type	Trap Option
%STKUNIT4-M:CP %CHMGR-1-PSU_FAN_STATUS: Fan 0 in PSU 1 of Unit 4 is up		
FANTRAY_OR_PSU_DOWN	ENVMON	FAN
%STKUNIT4-M:CP %CHMGR-2-FANTRAY_OR_PSU_DOWN: Major alarm: fan tray 3 or power supply 1 of unit 4 is missing or down		
FAN_TRAY_BAD	ENVMON	FAN
%STKUNIT4-M:CP %CHMGR-2-FAN_TRAY_BAD: Major alarm: fan tray 2 in unit 4 is missing or down		
FAN_TRAY_OK	ENVMON	FAN
%STKUNIT4-M:CP %CHMGR-5-FAN_TRAY_OK: Major alarm cleared: fan tray 2 in unit 4 present		
FAN_BAD	ENVMON	FAN
%STKUNIT4-M:CP %CHMGR-2-FAN_BAD: Minor alarm: 1 out of 4 fans in fantray 1 of unit 4 are down		
TME_TASK_SUSPEND	ENVMON	NONE
%TME-2-TASK SUSPENDED: SUSPENDED - svce:%d - inst:%d - task:%s		
TME_TASK_TERM	ENVMON	NONE
%TME-2-ABNORMAL_TASK_TERMINATION: CRASH - task:%s %s		
CHM_CPU_THRESHOLD	ENVMON	NONE
%CHMGR-5-CPU_THRESHOLD: Cpu %s usage above threshold. Cpu5SecUsage (%d)		
CHM_CPU_THRESHOLD_CLR	ENVMON	NONE
%CHMGR-5-CPU_THRESHOLD_CLR: Cpu %s usage drops below threshold. Cpu5SecUsage (%d)		
CHM_MEM_THRESHOLD	ENVMON	NONE
%CHMGR-5-MEM_THRESHOLD: Memory %s usage above threshold. MemUsage (%d)		
CHM_MEM_THRESHOLD_CLR	ENVMON	NONE
%CHMGR-5-MEM_THRESHOLD_CLR: Memory %s usage drops below threshold. MemUsage (%d)		
MACMGR_STN_MOVE	ENVMON	NONE
%MACMGR-5-DETECT_STN_MOVE: Station Move threshold exceeded for Mac %s in vlan %d		
VRRP_BADAUTH	PROTO	NONE
%STKUNIT1-M:CP %VRRP-3-VRRP_BAD_AUTH: vrid-1 on Gi 11/12 rcvd pkt with authentication type mismatch. %STKUNIT1-M:CP %VRRP-3-VRRP_BAD_AUTH: vrid-1 on Gi 11/12 rcvd pkt with authentication failure		
VRRP_GO_MASTER	PROTO	NONE
%VRRP-6-VRRP_MASTER: vrid-%d on %s entering MASTER		

Message ID	Trap Type	Trap Option
VRRP_PROTOCOL_ERROR	PROTO	NONE
VRRP_PROTOERR: VRRP protocol error on %S		
BGP4_ESTABLISHED	PROTO	NONE
%TRAP-5-PEER_ESTABLISHED: Neighbor %a, state %s		
BGP4_BACKW_XSITION	PROTO	NONE
%TRAP-5-BACKWARD_STATE_TRANS: Neighbor %a, state %s		
ETS_TRAP_TYPE_MODULE_STATUS_CHANGE	ETS	NONE
%DIFFSERV-5-ETS_TRAP_TYPE_MODULE_STATUS_CHANGE: ETS Module status changed to enabled %DIFFSERV-5-ETS_TRAP_TYPE_MODULE_STATUS_CHANGE: ETS Module status changed to disabled		
ETS_TRAP_TYPE_ADMIN_MODE_CHANGE	ETS	NONE
%DIFFSERV-5-ETS_TRAP_TYPE_ADMIN_MODE_CHANGE : ETS Admin mode changed to on for port %s %DIFFSERV-5-ETS_TRAP_TYPE_ADMIN_MODE_CHANGE : ETS Admin mode changed to off for port %s		
ETS_TRAP_TYPE_OPER_STATE_CHANGE	ETS	NONE
%DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to init for port %s %DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to off for port %s %DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to recommended for port %s %DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to rxConfigSrc for port %s		
ETS_TRAP_TYPE_PEER_STATE_CHANGE	ETS	NONE
%DIFFSERV-5-ETS_TRAP_TYPE_PEER_STATE_CHANGE : ETS Peer state changed to enabled for port %s %DIFFSERV-5-ETS_TRAP_TYPE_PEER_STATE_CHANGE : ETS Peer state changed to disabled for port %s		
PFC_TRAP_TYPE_MODULE_STATUS_CHANGE	PFC	NONE
%DIFFSERV-5-PFC_TRAP_TYPE_MODULE_STATUS_CHANGE: PFC Module status changed to enabled %DIFFSERV-5-PFC_TRAP_TYPE_MODULE_STATUS_CHANGE: PFC Module status changed to disabled		
PFC_TRAP_TYPE_ADMIN_MODE_CHANGE	PFC	NONE
%DIFFSERV-5-PFC_TRAP_TYPE_ADMIN_MODE_CHANGE : PFC Admin mode changed to on for port %s %DIFFSERV-5-PFC_TRAP_TYPE_ADMIN_MODE_CHANGE : PFC Admin mode changed to off for port %s		
PFC_TRAP_TYPE_OPER_STATE_CHANGE	PFC	NONE
%DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to init for port %s %DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to off for port %s %DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to recommended for port %s		

Message ID	Trap Type	Trap Option
`%DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to rxConfigSrc for port %s`		
PFC_TRAP_TYPE_PEER_STATE_CHANGE	PFC	NONE
`%DIFFSERV-5-PFC_TRAP_TYPE_PEER_STATE_CHANGE: PFC Peer state changed to enabled for port %s` `%DIFFSERV-5-PFC_TRAP_TYPE_PEER_STATE_CHANGE: PFC Peer state changed to disabled for port %s`		
FIPS_MAX_FCF_LIMIT_RCH	FIPS	NONE
`%FCOE-5-MAX_FCF_LIMIT_RCH: Number of FCFs reached maximum allowed limit in VLAN %d`		
FIPS_MAX_ENODE_LIMIT_RCH	FIPS	NONE
`%FCOE-5-MAX_ENODE_LIMIT_RCH: Number of ENodes reached maximum allowed limit in the system`		
FIPS_MAX_SESSION_LIMIT_RCH	FIPS	NONE
`%FCOE-5-MAX_SESSION_LIMIT_RCH: Number of sessions reached maximum allowed limit in the system`		
FIPS_FCF_DROP	FIPS	NONE
`%FCOE-5-FCF_DROP: New FCF(%d,%s) discovered in Vlan %d is dropped as max-FCF-limit per VLAN is reached`		
FIPS_ENODE_DROP	FIPS	NONE
`%FCOE-5-ENODE_DROP: New ENode(%d,%s) discovered in interface %s dropped as max-ENode-limit in system reached`		
FIPS_SESSION_DROP	FIPS	NONE
`%FCOE-5-SESSION_DROP: New session(%d,%s) request in interface %s dropped as max-session-limit in system reached`		
FIPS_ACL_INSTALL_FAIL	FIPS	NONE
`%FCOE-5-ACL_INSTALL_FAIL: problem in installing ACL entries due to no space or hardware failure`		
CHMGR_ENT_LAST_CHANGE_TIME	ENTITY	NONE
`No error messages. Time, at which there is a change in a physical entity, is logged.`		